Carlos Ivorra Castillo

EL ÁLGEBRA Y LA GEOMETRÍA ELEMENTAL

Para explicar el significado de la geometría pura podríamos usar la fórmula usual de exención de responsabilidades de las películas: No se pretende reflejar las características de las figuras geométricas o de las propiedades espaciales de cuerpos reales. Cualquier parecido entre los conceptos primitivos y sus connotaciones geométricas habituales es pura coincidencia.

CARL G. HEMPEL

Índice General

Introducción

El propósito de este libro es presentar dos teorías axiomáticas (y algunas teorías relacionadas) estrechamente vinculadas entre sí, a las que podríamos llamar el *Álgebra elemental,* y la *Geometría elemental,* porque en ellas se pueden formalizar prácticamente todos los resultados sobre el álgebra de los números reales y complejos (sin entrar en el cálculo diferencial) y la geometría euclídea clásica (sin llegar a argumentos "protoanalíticos" sobre pasos al límite en el cálculo de áreas, etc.)

Lo habitual es formalizar estos resultados en el seno de la teoría de conjuntos, y lo que hacen las teorías a las que nos referimos es independizar el álgebra y la geometría elemental de la teoría de conjuntos por una parte, pero también de la aritmética elemental por otra, pues el álgebra elemental no permite formalizar, por ejemplo, resultados como que todo número natural se descompone en producto de factores primos. Ése resultado es aritmético y no algebraico. De hecho, podríamos decir que el álgebra y la geometría elementales son esencialmente la porción del álgebra y de la geometría que es posible formalizar sin apoyarse en el aparato de la teoría de conjuntos y sin permitir que en ella puedan ser definidos los números naturales.

La ventaja de este doble aislamiento es que, por una parte —y al contrario de lo que sucede con la teoría de conjuntos— es posible demostrar que el álgebra y la geometría elemental son teorías consistentes y, por otra parte —al contrario de lo que sucede con la aritmética elemental— es posible demostrar que son completas. A su vez, esto implica que son decidibles: existe un algoritmo que determina en un número finito de pasos si una afirmación dada es demostrable o no en cualquiera de las dos teorías (si bien aplicarlo en la práctica requeriría tanto tiempo y tantos cálculos que no resulta viable).

Los resultados sobre completitud se deben a Tarski, al igual que la axiomática para la geometría euclídea que vamos a presentar aquí, que, al contrario que otras teorías axiomáticas, tiene la característica de emplear como términos primitivos únicamente los de "punto", "estar entre" y "ser congruente", de modo que todos los demás conceptos geométricos, incluyendo los de "recta", "plano" y, en general, el de "variedad de dimensión n", se definen a partir de éstos.

Este libro es esencialmente autocontenido, en el sentido de que sólo requiere del lector un conocimiento de lo que es un lenguaje formal y una teoría axiomática de primer orden. Sólo en un momento dado, en la prueba de la consistencia del álgebra elemental, necesitaremos un resultado técnico no trivial que

se demuestra utilizando el teorema de eliminación de cortes libres en el cálculo secuencial de Gentzen, para el que el lector será remitido a mi libro de *Lógica Matemática.* En algunos resultados secundarios, completamente prescindibles para los objetivos principales de este libro, remitiré a algunas propiedades sobre los cuerpos realmente cerrados demostradas en mi libro de *Álgebra.*

Toda teoría axiomática tiene limitaciones en su capacidad expresiva (en el sentido de que hay afirmaciones no formalizables en ella), pero en el caso de la teoría de conjuntos estas limitaciones quedan muy lejos de los enunciados que manejan la mayor parte de los matemáticos, y sólo requieren atención en áreas muy particulares en las que las clases propias representan un papel destacado, como la teoría de categorías o la teoría de conjuntos como especialidad matemática. En cambio, en este libro vamos a tener que explotar al máximo la capacidad expresiva de las teorías que vamos a manejar, especialmente en la parte del álgebra elemental, por lo que la principal preocupación del lector debería ser convencerse de que en ningún momento la estamos rebasando, de modo que todos los enunciados y razonamientos son realmente formalizables en el marco de trabajo considerado.

En el primer capítulo hemos incluido numerosas notas al pie con la intención de aclarar los puntos en los que esta posibilidad podría resultar dudosa. El problema principal es que no es posible mostrar explícitamente el modo en que los distintos enunciados y razonamientos se formalizan en las teorías consideradas porque ello llevaría a fórmulas inmanejables por su longitud y complejidad, por lo que en general tendremos que contentarnos con entender conceptualmente cómo se podrían escribir esas fórmulas sin necesidad de pararnos a escribirlas explícitamente.

Por otra parte, en la página 74 hemos incluido un ejemplo de la clase de razonamientos incorrectos a los que se puede llegar si no se tienen en cuenta las limitaciones de expresividad de las teorías que estamos considerando. Confiamos en que las notas y este ejemplo puedan bastar al lector para hacerse una idea exacta de las posibilidades reales de las teorías consideradas.

Primera parte

El álgebra elemental

Capítulo I

La teoría elemental de cuerpos

En este primer capítulo estudiaremos las consecuencias de los meros axiomas que en la teoría de conjuntos se usan para definir la estructura algebraica de cuerpo o, dicho de otro modo, las propiedades generales de la suma y del producto. La principal ausencia será la relación de orden, que interviene igualmente en las manipulaciones algebraicas que podemos englobar en el "álgebra elemental". En el capítulo siguiente veremos el impacto que tiene su introducción sobre la teoría.

Dado que no contamos con el apoyo de la teoría de conjuntos, dedicamos la primera sección a mostrar en general, cómo es posible utilizar parcialmente el lenguaje conjuntista en cualquier teoría axiomática.

1.1 La lógica de clases

Consideremos cualquier teoría axiomática sobre un lenguaje formal $\mathcal{L}$. Convenimos en que sus signos lógicos no definidos son $\neg, \rightarrow, \bigwedge, =$ y las variables. Usaremos la notación

$$\bigvee_{i=1}^{n} \alpha_i \equiv \alpha_1 \vee \cdots \vee \alpha_n, \qquad \bigwedge_{i=1}^{n} \alpha_i \equiv \alpha_1 \wedge \cdots \wedge \alpha_n$$

para representar disyunciones y conjunciones de n fórmulas.

Multitérminos Una de las características de la teoría de conjuntos es que permite definir pares, ternas, cuádruplas, etc. de conjuntos, de manera que todo par de objetos de la teoría (todo par de conjuntos) está codificado por un tercer objeto (el par ordenado formado por dos conjuntos es un tercer conjunto). Esto no va a ser así en las teorías que vamos a manejar, pero nada nos impide "hablar en bloque" de varios objetos, lo cual en la práctica es equivalente a hablar de

pares, ternas, etc. de objetos. Para ello es conveniente introducir una notación adecuada.

Para cada número natural $n \geq 1$, usaremos la notación $\bar{t}_n$ (o simplemente $\bar{t}$, cuando n sea conocido o sea irrelevante) para indicar que la letra $\bar{t}$ no representa a un término de $\mathcal{L}$, sino a un *"multitérmino"*, es decir, a una sucesión de n términos $\bar{t}_n \equiv (t_1, \ldots, t_n)$.

En principio, esto no es más que un convenio metamatemático (somos libres de dar cualquier nombre a cualquier cosa, y nada nos impide dar nombres a las sucesiones de n términos de un lenguaje formal), pero a partir de él obtenemos un convenio para nombrar determinadas fórmulas de $\mathcal{L}$. Por ejemplo, si $\bar{t}_n$ y $\bar{t}'_n$ son dos multitérminos de la misma longitud, podemos convenir que

$$\bar{t}_n = \bar{t}'_n \equiv t_1 = t'_1 \land \cdots \land t_n \equiv t'_n,$$

de modo que $\bar{t}_n = \bar{t}'_n$ se refiere a una fórmula de $\mathcal{L}$.

Si $\bar{v}_n$ es una *"multivariable"* (es decir, un multitérmino cuyas componentes son todas variables), usaremos $\bigwedge \bar{v}_n$ y $\bigvee \bar{v}_n$ para abreviar $\bigwedge v_1 \cdots v_n$ y $\bigvee v_1 \cdots v_n$, respectivamente. Así, por ejemplo,

$$\bigwedge \bar{v}_2 \bar{w}_2 (\bar{v}_2 = \bar{w}_2 \leftrightarrow \bar{w}_2 = \bar{v}_2)$$

representa a una sentencia de $\mathcal{L}$, que podemos concebir como que expresa que la igualdad de pares ordenados es simétrica, si bien no hemos definido, ni vamos a definir en ningún momento, el concepto de par ordenado.

Clases Si $\phi(\bar{v}_m, \bar{w}_n)$ es cualquier fórmula de $\mathcal{L}$ cuyas variables libres estén entre las indicadas (es decir, entre $v_1, \ldots, v_m, w_1, \ldots, w_n$), usaremos la notación

$$A_m = \{\bar{v}_m \mid \phi(\bar{v}_m, \bar{w}_n)\},$$

y leeremos que "A_m es la *clase* de todas las m-tuplas $\bar{v}_m$ que cumplen $\phi(\bar{v}_m, \bar{w}_n)$" que, en sí misma, no significa nada, pero que servirá de "código" para interpretar determinados nombres de fórmulas de $\mathcal{L}$. Por ejemplo, convendremos en que

$$\bar{v}_m \in A_m \equiv \phi(\bar{v}_m, \bar{w}_n), \qquad \bar{v}_m \notin A_m \equiv \neg\phi(\bar{v}_m, \bar{w}_n).$$

Así, no es necesario tener una respuesta a la pregunta "¿Qué es A_m exactamente?" para que podamos afirmar que $\bar{v}_m \in A_m$ representa inequívocamente a la fórmula $\phi(\bar{v}_m, \bar{w}_n)$.

Igualmente, si hemos definido de este modo dos clases de m-tuplas A_m y B_m, convendremos en que

$$A_m = B_m \equiv \bigwedge \bar{v}_m (\bar{v}_m \in A_m \leftrightarrow \bar{v}_m \in B_m) \equiv \bigwedge \bar{v}_m (\phi(\bar{v}_m, v_n) \leftrightarrow \psi(\bar{v}_m, \bar{x}_r)),$$

donde ψ es la fórmula que define a B_m. Diremos entonces que "la clase A_m es igual a la clase B_m", y lo importante es que esto tiene un significado preciso (representa una fórmula precisa de $\mathcal{L}$) sin necesidad de que las palabras "clase A_m" y "clase B_m" lo tengan.

También podemos definir la inclusión entre clases:

$$A_m \subset B_m \equiv \bigwedge \bar{v}_m(\bar{v}_m \in A_m \to \bar{v}_m \in B_m),$$

de modo que, por ejemplo, es un teorema lógico que

$$A_m = B_m \leftrightarrow A_m \subset B_m \land B_m \subset A_m.$$

Unas clases que siempre podemos definir son la *clase universal,* la *clase vacía:*

$$V = \{x \mid x = x\}, \qquad \varnothing = \{x \mid x \neq x\},$$

las clases finitas: $\{\bar{x}^1_m, \ldots, \bar{x}^n_m\} = \{\bar{v}_m \mid \bar{v}_m = \bar{x}^1_m \lor \cdots \lor \bar{v}_m = \bar{x}^n_m\}$, o las clases de m-tuplas:

$$V^m = \{\bar{v}_m \mid \bar{v}_m = \bar{v}_m\},$$

de modo que $\bar{v} \in V^m$ será otra forma de indicar que $\bar{v}$ es una multivariable de longitud m y $A \subset V^m$ será otra forma de indicar que A es una clase de m-tuplas.

A partir de unas clases pueden definirse otras, como la *unión,* la *intersección,* el *complemento* y la *diferencia* de clases:

$$A_m \cup B_m = \{\bar{v}_m \mid \bar{v}_m \in A_m \lor \bar{v}_m \in B_m\}, \; A_m \cap B_m = \{\bar{v}_m \mid \bar{v}_m \in A_m \land \bar{v}_m \in B_m\},$$

$$\bar{A}_m = \{\bar{v}_m \mid \bar{v}_m \notin A\}, \qquad \bar{A}_m \setminus \bar{B}_m \equiv \{\bar{v}_m \mid \bar{v}_m \in A_m \land \bar{v}_m \notin B_m\}.$$

Con estas definiciones, muchos teoremas de la teoría de conjuntos pueden reinterpretarse como teoremas sobre clases de cualquier teoría axiomática, como $A_m \cap B_m \subset A_m$, etc.

Si $\bar{t}_m$ y $\bar{t}'_n$ son multitérminos, representaremos por $(\bar{t}_m, \bar{t}'_n)$ el multitérmino de longitud $m+n$ que resulta de concatenarlos, de modo que, por ejemplo,

$$(\bar{t}_2, \bar{t}'_3) \equiv (t_1, t_2, t'_1, t'_2, t'_3).$$

Esto nos permite definir el *producto cartesiano* de clases:

$$A_m \times B_n = \{(\bar{v}_m, \bar{w}_n) \mid \bar{v}_m \in A_m \land \bar{w}_n \in B_n\}.$$

Diremos que una clase F es una *aplicación* de una clase A_m en otra B_n, y lo representaremos por $F : A_m \longrightarrow B_n$ si $F \subset A_m \times B_m$ y

$$\bigwedge \bar{v}_m \in A_m \overset{1}{\bigvee} \bar{w}_n \in B_n \; (\bar{v}_m, \bar{w}_n) \in F.$$

Usaremos la notación $\bar{F}(\bar{v}_m)$ para referirnos al único $\bar{w}_n$ que indica esta definición. Específicamente, esto se interpreta como que la notación $\bar{w}_n = F(\bar{v}_m)$ será una abreviatura para la fórmula $(\bar{v}_m, \bar{w}_m) \in F$.

Dadas dos aplicaciones $F : A_m \longrightarrow B_n$ y $G : B_n \longrightarrow C_r$, definimos su *composición* $F \circ G : A_m \longrightarrow C_r$ como la aplicación determinada por la relación $(F \circ G)(\bar{v}_m) = G(F(\bar{v}_m))$. Equivalentemente:

$$F \circ G = \{(\bar{v}_m, \bar{w}_r) \mid \bigvee \bar{x}_n((\bar{v}_m, \bar{x}_n) \in F \land (\bar{x}_n, \bar{w}_r) \in G)\}.$$

Omitimos las definiciones obvias de otros conceptos conjuntistas relacionados con las aplicaciones que sin duda el lector conocerá, como los de "aplicación inyectiva, suprayectiva, biyectiva", etc.

1.2 La teoría de cuerpos

El *lenguaje formal* (reducido) *del álgebra elemental* es el lenguaje $\mathcal{L}_A^-$ cuyos únicos signos eventuales son dos constantes $0, 1$, un funtor monádico $-$, y dos funtores diádicos $+$ y $\cdot$. En el capítulo siguiente definiremos un lenguaje $\mathcal{L}_A$ que contendrá un relator adicional para representar una relación de orden.

La *teoría de cuerpos elemental* es la teoría axiomática C sobre $\mathcal{L}_A^-$ determinada por los axiomas siguientes:

C1	$(x+y)+z = x+(y+z)$
C2	$x+y = y+x$
C3	$x+0 = x$
C4	$x+(-x) = 0$
C5	$(xy)z = x(yz)$
C6	$xy = yx$
C7	$x \cdot 1 = x$
C8	$x \neq 0 \rightarrow \bigvee y\ xy = 1$
C9	$x(y+z) = xy+xz$
C10	$0 \neq 1$

A los objetos de la teoría los llamaremos *"números"*, es decir, $\bigwedge x$ lo leeremos "para todo número x", mientras que $\bigvee x$ lo leeremos "existe un número x". Esto debe entenderse en un plano meramente informal, como una forma de facilitar la lectura de las fórmulas de $\mathcal{L}_A^-$, exactamente en el mismo sentido que consideramos que el lenguaje de la teoría de conjuntos habla sobre unos "conjuntos" que en ningún momento se definen.

Si $x_1, x_2, \ldots$ son variables de $\mathcal{L}_A^-$, definimos recurrentemente

$$\sum_{i=1}^{1} x_i = x_1, \qquad \sum_{i=1}^{n+1} x_i = \sum_{i=1}^{n} x_i + x_{n+1},$$

de modo que, por ejemplo,

$$\sum_{i=1}^{5} x_i = (((x_1+x_2)+x_3)+x_4)+x_5.$$

A menudo usaremos la notación alternativa

$$x_1+\cdots+x_n \equiv \sum_{i=1}^{n} x_i.$$

En general, $\sum_{i=1}^{n} x_i$ es un término con las variables libres $x_1, \ldots, x_n$, que a su vez pueden ser sustituidas por términos cualesquiera $t_1, \ldots, t_n$, lo que da lugar a términos que representaremos por $\sum_{i=1}^{n} t_i \equiv t_1+\cdots+t_n$.

Convendremos en que $\sum_{i=1}^{0} x_i \equiv 0$.

El teorema siguiente expresa la propiedad asociativa generalizada:[1]

Teorema 1.1 $\sum\limits_{i=1}^{m+n} x_i = \sum\limits_{i=1}^{m} x_i + \sum\limits_{i=1}^{n} x_{m+i}.$

DEMOSTRACIÓN: Por inducción sobre n. Para $n = 0$ se trata del axioma **C3**. Si se cumple para n, entonces

$$\sum_{i=1}^{m+n+1} x_i = \sum_{i=1}^{m+n} x_i + x_{m+n+1} = (\sum_{i=1}^{m} x_i + \sum_{i=1}^{n} x_{m+i}) + x_{m+n+1} =$$

$$\sum_{i=1}^{m} x_i + (\sum_{i=1}^{n} x_{m+i} + x_{m+n+1}) = \sum_{i=1}^{m} x_i + \sum_{i=1}^{n+1} x_{m+i},$$

donde hemos usado **C1**. ■

Es pura rutina demostrar la propiedad conmutativa generalizada:

Teorema 1.2 *Si σ es cualquier permutación de los índices $1, \ldots, n$, se cumple:*

$$\sum_{i=1}^{n} x_{\sigma i} = \sum_{i=1}^{n} x_i.$$

DEMOSTRACIÓN: Por inducción sobre n. Para $n = 1$ no hay nada que probar.

Supongamos que el resultado es cierto para n y sea i el índice que cumple $\sigma i = n + 1$. Entonces, usando el teorema anterior y **C2** vemos que

$$x_{\sigma 1} + \cdots + x_{\sigma n} = (x_{\sigma 1} + \cdots + x_{\sigma(i-1)}) + (x_{n+1} + (x_{\sigma(i+1)} + \cdots + x_{\sigma n}))$$

$$= (x_{\sigma 1} + \cdots + x_{\sigma(i-1)}) + ((x_{\sigma(i+1)} + \cdots + x_{\sigma n}) + x_{n+1})$$

$$= (x_{\sigma 1} + \cdots + x_{\sigma(i-1)} + x_{\sigma(i+1)} + \cdots + x_{\sigma n}) + x_{n+1},$$

El primer sumando del último término es una permutación de $x_1 + \cdots + x_n$, luego por hipótesis de inducción puede probarse que es igual a $x_1 + \cdots + x_n$, lo que nos da la conclusión. ■

Este resultado justifica que definamos sumatorios en los que no se especifique el orden de las variables. A la hora de traducir tales sumatorios en términos concretos de $\mathcal{L}_A^-$ habrá que elegir un orden en particular, pero no es necesario

---

[1]Observemos que en una expresión de la forma $\sum\limits_{i=1}^{n} x_i$, el número natural n es siempre un número natural metamatemático, de modo que, por ejemplo, el teorema 1.1 es un esquema teoremático en C, es decir, una serie de infinitos teoremas de C, uno para cada valor posibles de m y n. Por ejemplo, un caso particular es

$$x_1 + x_2 + x_3 + x_4 + x_5 = (x_1 + x_2 + x_3) + (x_4 + x_5).$$

Todas las pruebas de esquemas teoremáticos que vamos a dar son constructivas, en el sentido de que un análisis minucioso permite convertirlas en algoritmos para generar una demostración de cada caso particular del esquema.

dar detalles que especifiquen ninguna elección porque ésta es irrelevante. Un ejemplo lo tenemos en la propiedad distributiva generalizada:

$$\Big(\sum_{i=1}^{m} x_i\Big)\Big(\sum_{j=1}^{n} y_j\Big) = \sum_{i,j} x_i y_j,$$

donde en el segundo sumatorio hay que entender que se suman todos los términos $x_i y_j$ donde i, j recorren todos los valores posibles $1 \leq i \leq m$, $1 \leq j \leq n$, pero no es necesario especificar en qué orden hay que escribir tales términos.

Esta propiedad se demuestra sin dificultad por inducción sobre m, y el caso $m = 1$, que tiene interés por sí mismo:

$$x(y_1 + \cdots + y_n) = xy_1 + \cdots + xy_n$$

se demuestra a su vez por inducción sobre n.

Similarmente podemos definir

$$\prod_{i=1}^{1} x_i = x_1, \quad \prod_{i=1}^{n+1} x_i = \prod_{i=1}^{n} x_i \cdot x_{n+1},$$

con el convenio de que $\prod\limits_{i=1}^{0} x_i = 1$. Escribiremos también

$$x_1 \cdots x_n \equiv \prod_{i=1}^{n} x_i.$$

Las propiedades asociativa y conmutativa generalizadas se demuestran para el producto exactamente igual que para la suma, usando ahora los axiomas **C5**, **C6** y **C7**.

En general, a partir de aquí manejaremos libremente las sumas y productos finitos, dando por hecho que cualquier manipulación considerada se justifica fácilmente por inducción.

Conviene observar que 0 y 1 son los únicos números que cumplen los axiomas **C3** y **C7**, respectivamente, es decir, que

$$\bigwedge x(x + y = x) \rightarrow y = 0, \qquad \bigwedge x(x \cdot y = x) \rightarrow y = 1.$$

En efecto, basta sustituir $x = 0$ en la hipótesis de la primera fórmula y obtenemos $0 + y = 0$, luego $y = 0$, y análogamente se justifica la segunda,

Similarmente, $-x$ es el único número que cumple el axioma **C4**:

$$x + y = 0 \rightarrow y = -x.$$

En efecto:

$$y = y + 0 = y + (x + (-x)) = (y + x) + (-x) = 0 + (-x) = -x.$$

Diremos que $-x$ es el *opuesto* de x. Escribiremos $x - y$ en lugar de $x + (-y)$.

El axioma **C8** afirma que todo número no nulo tiene un *inverso* y un razonamiento totalmente análogo al anterior prueba que es único. Definimos $x^{-1} \equiv y \mid x \cdot y = 1$, de modo que si $x \neq 0$ se cumple que $x \cdot x^{-1} = 1$.

Notemos que, por conveniencia, hemos convertido a $-$ en un término primitivo del lenguaje $\mathcal{L}_A^-$, mientras que a $(\ )^{-1}$ lo consideramos un concepto definido. Escribiremos x/y en lugar de xy^{-1}. En particular, $x^{-1} = 1/x$.

He aquí las propiedades algebraicas más básicas:

Teorema 1.3 *Se cumple:*

1. $-(-x) = x$,
2. $x \neq 0 \rightarrow (x^{-1})^{-1} = x$,
3. $x \cdot 0 = 0$,
4. $xy = 0 \rightarrow x = 0 \vee y = 0$,
5. $(-x)y = x(-y) = -(xy)$,
6. $(-x)(-y) = xy$.

DEMOSTRACIÓN: 1. Basta observar que $-x + x = 0$, lo cual significa que x es el opuesto de $-x$. La prueba de 2) es análoga.

3. $x \cdot 0 + x \cdot 0 = x(0 + 0) = x \cdot 0$, luego $x \cdot 0 = x \cdot 0 - (x \cdot 0) = 0$.

4. Si $xy = 0$ pero $x \neq 0$, entonces $x^{-1}xy = x^{-1} \cdot 0 = 0$, luego $y = 0$.

5. $xy + (-x)y = (x - x)y = 0 \cdot y = 0$, luego $(-x)y$ es el opuesto de xy. La otra igualdad se prueba análogamente.

6. $(-x)(-y) = -(x(-y)) = -(-(xy)) = xy$. ■

La propiedad 3. explica por qué hay que exceptuar el 0 en la existencia de inversos. Por otra parte, ahora es claro que

$$x \pm y = z \rightarrow x = z \mp y,$$

es decir, que en C podemos despejar sumandos en igualdades de la forma habitual. En particular, podemos simplificarlos:

$$x + z = y + z \rightarrow x = y.$$

Lo mismo vale para productos, con el único cuidado de no dividir entre 0:

$$x \neq 0 \wedge xy = z \rightarrow y = z/x, \qquad x \neq 0 \wedge xy = xz \rightarrow y = z.$$

Notemos también que, por la propiedad 5, se cumple $-x = (-1)x$, por lo que los signos quedan regulados por las propiedades usuales del producto. Por ejemplo, $-(x + y) = -x - y$ es simplemente un caso particular de la propiedad distributiva.

También es fácil demostrar ahora las reglas usuales para operar con fracciones:

$$\frac{x}{y}=\frac{z}{w}\leftrightarrow xw=yz, \qquad \frac{x}{y}+\frac{z}{w}=\frac{xw+yz}{yw}, \qquad \frac{x}{y}\cdot\frac{z}{w}=\frac{xz}{yw},$$

$$x=\frac{x}{1}, \qquad -\frac{x}{y}=\frac{-x}{y}=\frac{x}{-y}, \qquad \left(\frac{x}{y}\right)^{-1}=\frac{y}{x}, \qquad \frac{x/y}{z/w}=\frac{xw}{yz},$$

donde todas las igualdades requieren como hipótesis que los denominadores que intervienen no sean nulos.

Si m es un número entero (metamatemático) usaremos la notación

$$mx=\begin{cases}\overbrace{x+\cdots+x}^{m \text{ veces}} & \text{si } m>0,\\ 0 & \text{si } m=0,\\ \overbrace{-x\cdots-x}^{-m \text{ veces}} & \text{si } m<0,\end{cases} \qquad x^m=\begin{cases}\overbrace{x\cdots x}^{m \text{ veces}} & \text{si } m>0,\\ 1 & \text{si } m=0,\\ \overbrace{x^{-1}\cdots x^{-1}}^{-m \text{ veces}} & \text{si } m<0,\end{cases}$$

donde la definición de x^m requiere $x\neq 0$ cuando m es negativo.

Es fácil demostrar inductivamente las propiedades "naturales" de estas operaciones:

$$m(x+y)=mx+my, \quad (m+n)x=mx+nx, \quad (xy)^m=x^my^m, \quad x^{m+n}=x^my^n,$$

$$m(nx)=(mn)x, \qquad (x^m)^n=x^{mn}$$

$$0x=0, \quad m0=0, \quad x^1=x, \quad 1^m=1, \quad 0^m=0,$$

donde la última propiedad requiere que $m>0$ y, en general, las bases tienen que ser no nulas cuando los exponentes son negativos.

Notemos que, en principio, mx es una operación externa, en el sentido de que estamos multiplicando un número entero metamatemático por un número de la teoría formal. Sin embargo, no es necesario considerarlo así, ya que podemos identificar el entero metamatemático m con el número formal $m\cdot 1$, y entonces $mx=(m1)x$ es el producto de dos números de la teoría formal. Las propiedades precedentes permiten demostrar fácilmente en C cualquier suma o producto de números enteros. Por ejemplo,

$$2+3=5, \qquad 7\cdot 3=21, \quad \ldots$$

son ejemplos de teoremas de C. El primero es, más detalladamente:

$$(1+1)+(1+1+1)=1+1+1+1+1.$$

En cambio, la exponenciación x^n sí que es una operación externa, en la que un número de la teoría formal se opera con un entero metamatemático.

Hay que tener presente que, al interpretar los enteros como números de la teoría formal, no podemos demostrar,[2] digamos, que $7\neq 12$.

[2]La razón es que hay cuerpos que cumplen todos los axiomas (luego todos los teoremas) de C y en los cuales $7=12$.

Para garantizar que los enteros formalizados se corresponden biunívocamente con los enteros metamatemáticos necesitamos incorporar un axioma o, más precisamente un esquema axiomático:

La *teoría de los cuerpos de característica* 0 es la teoría axiomática C_0 que resulta de añadir a los axiomas de C el esquema axiomático siguiente:

Car0 *Para todo número natural* $n > 0$*, la fórmula* $n \cdot 1 \neq 0$ *es un axioma.*

Así, si $m < n$ son dos números naturales, en C_0 se demuestra que $m \neq n$ (pues si suponemos $m = n$ llegamos a que $n - m = 0$, en contradicción con el axioma **Car0**).

En particular, para cada número racional $r = m/n$ (donde la fracción es irreducible), podemos definir el término $r \cdot 1 \equiv \frac{m\cdot 1}{n \cdot 1}$, y se comprueba inmediatamente que

$$\frac{m}{n} \cdot 1 = \frac{m \cdot 1}{n \cdot 1},$$

donde ahora no es necesario que la fracción sea irreducible, así como que si $r+s = t$, $rs = u$ son números racionales, entonces $\vdash_{\mathrm{C}_0} (r+s = t)$ y $\vdash_{\mathrm{C}_0} (rs = u)$.

En la práctica es como si en C_0 tuviéramos una constante para nombrar a cada número racional.

Alternativamente, si p es un número primo, podemos considerar la teoría C_p que resulta de añadir a C el axioma[3] **Car p** $\equiv p \cdot 1 = 0$.

Una teoría más débil que C_0 es la teoría $\mathrm{C}[\infty]$ que resulta de añadir a C el esquema axiomático de infinitud:

Inf *Para todo número natural* $n > 0$*, la fórmula*

$$\bigvee x_1 \cdots x_n \bigwedge_{i \neq j} x_i \neq x_j$$

es un axioma.

Es obvio que **Car0** implica **Inf,** pues el axioma n-simo de infinitud se cumple tomando $x_1 = 1, \ldots, x_n = n$.

A su vez, la alternativa al axioma de infinitud consiste en postular que el cuerpo de trabajo es finito. Concretamente, si p es un primo y n es un número natural no nulo, llamamos $\mathrm{C}[p^n]$ a la teoría que resulta de añadir a C el axioma

Card p^n $\bigvee x_1 \cdots x_{p^n} (\bigwedge_{i \neq j} x_i \neq x_j \land \bigwedge x \bigvee_{i=1}^{p^n} x = x_i)$.

Puede probarse que este axioma sería contradictorio para números naturales que no fueran potencia de primo, así como que **Card p^n** implica **Car p**.

Nosotros no entraremos en estos resultados porque nos va a interesar exclusivamente la teoría de los cuerpos infinitos de característica 0.

---

[3] Si p no es primo y tomamos este axioma, podemos considerar la descomposición en primos $p = p_1^{n_1} \cdots p_k^{n_k}$, y tenemos que $(p_1^{n_1} \cdot 1) \cdots (p_n^{n_k} \cdot 1) = 0$, de donde se sigue la disyunción **Car** $\mathbf{p}_1 \lor \cdots \lor$ **Car** $\mathbf{p}_k$.

1.3 Álgebra lineal

Al trabajar en la teoría C, usaremos la letra k para representar a la clase universal, en lugar de la V genérica que hemos empleado en la sección 1.1. Consecuentemente, a la clase de las n-tuplas de números la representaremos por k^n. En lugar de hablar de n-tuplas, hablaremos de *"vectores"* de n componentes. Para referirse a los números por oposición a los vectores es costumbre llamarlos *"escalares"*.

Insistimos en que, en este contexto, no existe ninguna definición de "vector", ni formalizada en C ni metamatemática. Simplemente, "vector de n componentes" es una expresión que emplearemos para leer ciertas fórmulas de $\mathcal{L}_A^-$ en las que ciertas variables sean tratadas sistemáticamente en bloques de n.

En toda esta sección consideraremos exclusivamente vectores de un número de componentes n fijo, por lo que habitualmente lo omitiremos y escribiremos $\bar{v}$ en lugar de $\bar{v}_n$.

Las constantes 0, 1 de $\mathcal{L}_A^-$ nos permiten definir los multitérminos

$$\bar{0} = (0, \ldots, 0), \qquad \bar{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0),$$

donde hay que entender que el 1 de $\bar{e}_i$ figura en la posición i-ésima.

Ahora definimos aplicaciones:

$$+ : k^n \times k^n \longrightarrow k^n, \qquad \cdot : k \times k^n \longrightarrow k^n$$

mediante

$$\bar{v} + \bar{w} \equiv (v_1 + w_1, \ldots, v_n + w_n), \qquad a\bar{v} = (av_1, \ldots, av_n).$$

Definimos también $-\bar{v} = (-v_1, \ldots, -v_n)$.

El significado preciso de estas definiciones consiste en que, por ejemplo, permiten interpretar inequívocamente como fórmulas precisas de $\mathcal{L}_A^-$ los distintos apartados del teorema siguiente, que se demuestra sin dificultad:

Teorema 1.4 *Se cumple:*[4]

1. $(\bar{v} + \bar{w}) + \bar{x} = \bar{v} + (\bar{w} + \bar{x})$,
2. $\bar{v} + \bar{w} = \bar{w} + \bar{v}$,
3. $\bar{v} + \bar{0} = \bar{v}$,
4. $\bar{v} + (-\bar{v}) = \bar{0}$,

[4] Cada afirmación de este teorema es un esquema teoremático con un caso particular para cada posible valor de n. Por ejemplo, la propiedad 2. incluye a las fórmulas de $\mathcal{L}_A^-$:

$$\bigwedge v_1 \cdots v_n w_1 \cdots w_n (v_1 + w_1 = w_1 + v_1 \land \cdots \land v_n + w_n = w_n + v_n),$$

que ciertamente se demuestras en C a partir del axioma **C2**.

5. $a(\bar{v}+\bar{w}) = a\bar{v}+a\bar{w}$,
6. $(a+b)\bar{v} = a\bar{v}+b\bar{v}$,
7. $a(b\bar{v}) = (ab)\bar{v}$,
8. $1\cdot\bar{v} = \bar{v}$.

Definición 1.5 Un *k-espacio vectorial* es una clase en la que hay definida una suma y un producto por escalares que cumplen las afirmaciones del teorema anterior.

En estos términos hemos demostrado que las operaciones que hemos definido en la clase k^n la convierten en un espacio vectorial. En lo sucesivo marcaremos con (EV) los teoremas y definiciones que dependan exclusivamente de dichos axiomas, sin tener en cuenta el hecho de que los vectores considerados son los de k^n en particular.

Teorema 1.6 (EV) *Se cumple:*

1. $a\cdot\bar{0} = \bar{0}$,
2. $0\cdot\bar{v} = \bar{0}$,
3. $a\bar{v} = \bar{0} \to a = 0 \lor \bar{v} = \bar{0}$,
4. $(-a)\bar{v} = a(-\bar{v}) = -(a\bar{v})$,
5. $a\bar{v} = a\bar{w} \land a \neq 0 \to \bar{v} = \bar{w}$,
6. $a\bar{v} = b\bar{v} \land \bar{v} \neq \bar{0} \to a = b$.

DEMOSTRACIÓN: 1. Tenemos que $a\cdot\bar{0} = a\cdot(\bar{0}+\bar{0}) = a\cdot\bar{0}+a\cdot\bar{0}$, luego sumando $-(a\cdot\bar{0})$ a ambos miembros llegamos a que $\bar{0} = a\cdot\bar{0}$.

2. se prueba análogamente. Para probar 3. suponemos $a \neq 0$, con lo que $a\bar{v} = 0$ implica que $a^{-1}(a\bar{v}) = a^{-1}\bar{0} = \bar{0}$, lo cual equivale a $(a^{-1}a)\bar{v} = \bar{0}$, o a $1\cdot\bar{v} = 0$, luego a $\bar{v} = 0$.

4. Partimos de que $\bar{0} = 0\cdot\bar{v} = (a+(-a))\bar{v} = a\bar{v}+(-a)\bar{v}$, luego sumando $-(a\bar{v})$ a ambos miembros queda $-(a\bar{v}) = (-a)\bar{v}$. La otra igualdad se prueba análogamente.

5. y 6. se reducen a 3. ■

Definimos

$$\sum_{i=1}^{1} \bar{v}_i = v_1, \qquad \sum_{i=1}^{n+1} \bar{v}_i \equiv \sum_{i=1}^{n} \bar{v}_i + \bar{v}_{i+1},$$

con el convenio adicional de que $\sum\limits_{i=1}^{0} \bar{v}_i = \bar{0}$. A menudo escribiremos $\bar{v}_1+\cdots+\bar{v}_n$ en lugar de un sumatorio de vectores. Los mismos argumentos empleados en las demostraciones de los teoremas 1.1 y 1.2 permiten probar las propiedades asociativa generalizada, conmutativa generalizada y distributiva generalizada respecto del producto por escalares. Por ello a partir de aquí usaremos las sumas finitas de vectores con la misma libertad que usamos las de números.

Pasamos ahora a considerar clases de vectores. Adoptaremos el convenio de representar por $0 \equiv \{\bar{0}\}$ a la clase cuyo único elemento es el vector $\bar{0}$ (que no debe ser confundida con el escalar 0).

Definición 1.7 (EV) Una clase de vectores $V \subset k^n$ es una *variedad lineal* si cumple las propiedades siguientes:

1. $\bar{0} \in V$,
2. $\bar{v} \in V \land \bar{w} \in V \to \bar{v} + \bar{w} \in V$,
3. $\bar{v} \in V \to a\bar{v} \in V$.

Por ejemplo, es inmediato probar que 0 y k^n son variedades lineales. Cuando V y W son variedades lineales, es costumbre escribir $V \leq W$ en lugar de $V \subset W$.

Definimos la *envoltura lineal* de unos vectores $\bar{v}_1, \ldots, \bar{v}_r$ como la clase[5]

$$\langle \bar{v}_1, \ldots, \bar{v}_r \rangle = \{\bar{v} \mid \bigvee a_1 \cdots a_r \ \bar{v} = a_1\bar{v}_1 + \cdots + a_r\bar{v}_r\}.$$

A sus elementos los llamaremos *combinaciones lineales* de $\bar{v}_1, \ldots, \bar{v}_r$".

Teorema 1.8 (EV) *La envoltura lineal $V = \langle \bar{v}_1, \ldots, \bar{v}_r \rangle$ de unos vectores dados es una variedad lineal que los contiene. Además, si W es una variedad lineal y $\bar{v}_1, \ldots, \bar{v}_r \in W$, entonces $V \leq W$.*

Demostración: La primera parte del teorema significa, más explícitamente, que se cumple lo siguiente:

1. $\bar{0} \in V$,
2. $\bar{v} \in V \land \bar{w} \in V \to \bar{v} + \bar{w} \in V$,
3. $\bar{v} \in V \to a\bar{v} \in V$.

La demostración es muy simple:

$$\bar{0} = 0 \cdot \bar{v}_1 + \cdots + 0 \cdot \bar{v}_r,$$

luego $\bar{0} \in V$. (El vector nulo es combinación lineal de cualquier clase de vectores.) Si $\bar{v} \in V$ y $\bar{v} \in V$, existen $a_1, \ldots, a_r, b_1, \ldots, b_r$ tales que

$$\bar{v} = a_1\bar{v}_1 + \cdots + a_r\bar{v}_r, \quad \bar{w} = b_1\bar{v}_1 + \cdots + b_r\bar{v}_r,$$

luego

$$\bar{v} + \bar{w} = (a_1 + b_1)\bar{v}_1 + \cdots + (a_r + b_r)\bar{v}_r \in V.$$

La tercera propiedad se demuestra de forma similar.

[5]Esto significa que $\bar{v} \in \langle \bar{v}_1, \ldots, \bar{v}_r \rangle$ es, por definición, una abreviatura de la fórmula de $\mathcal{L}_A^-$

$$\bigvee a_1 \cdots a_r \ \bar{v} = a_1\bar{v}_1 + \cdots + a_r\bar{v}_r.$$

Que V contiene a $\bar{v}_1, \ldots, \bar{v}_r$ significa que $\bar{v}_i \in V$, lo cual es cierto, pues basta definir $a_i = 1$ y $a_j = 0$, para $j \neq i$, y entonces $v_i = a_1\bar{v}_1 + \cdots + a_n\bar{v}_r \in V$.

Si W es una variedad lineal que contiene a $\bar{v}_1, \ldots, \bar{v}_r$, tomamos $\bar{v} \in V$, de modo que existen $a_1, \ldots, a_r$ tales que $\bar{v} = a_1\bar{v}_1 + \cdots + a_r\bar{v}_r$, y entonces $\bar{a}_i\bar{v}_i \in W$ por la tercera propiedad de la definición de variedad lineal, y una simple inducción sobre r basada en la segunda propiedad nos da que $\bar{v} \in W$. ■

Definición 1.9 (EV) Diremos que unos vectores $\bar{v}_1, \ldots, \bar{v}_r$ son *linealmente independientes* o que forman un *sistema libre* si

$$\bigwedge a_1 \cdots a_r(a_1\bar{v}_1 + \cdots + a_r\bar{v}_r = \bar{0} \to a_1 = 0 \land \cdots \land a_r = 0).$$

En caso contrario diremos que son *linealmente dependientes,* o que forman un *sistema ligado.*

Ejemplo *Los vectores $\bar{e}_1, \ldots, \bar{e}_n$ son linealmente independientes.*

En efecto, si $a_1\bar{e}_1 + \cdots + a_n\bar{e}_n = \bar{0}$, esto equivale a que $(a_1, \ldots, a_n) = \bar{0}$, que a su vez equivale a que $a_1 = 0 \land \cdots \land a_n = 0$. ■

Veamos una caracterización:

Teorema 1.10 (EV) *Unos vectores $\bar{v}_1, \ldots, \bar{v}_r$ (que no se reduzcan al vector $\bar{0}$) son linealmente dependientes si y sólo si existe*[6] *un i tal que $\bar{v}_i$ es combinación lineal de $\bar{v}_1, \ldots, \bar{v}_{i-1}, \bar{v}_{i+1}, \ldots \bar{v}_r$.*

Demostración: El caso $r = 1$ se trata aparte y es trivial. A partir de aquí suponemos $r \geq 2$.

Si los vectores son linealmente dependientes, por definición existen $a_1, \ldots, a_r$ tales que $a_1\bar{v}_1 + \cdots + a_r\bar{v}_r = \bar{0}$ y $a_1 \neq 0 \lor \cdots \lor a_r \neq 0$. Si es $a_i \neq 0$, entonces

$$\bar{v}_i = -\frac{a_1}{a_i}\bar{v}_1 - \cdots - \frac{a_{i-1}}{a_i}\bar{v}_{i-1} - \frac{a_{i+1}}{a_i}\bar{v}_{i+1} - \cdots - \frac{a_r}{a_i}\bar{v}_r.$$

Recíprocamente, si $\bar{v}_i$ es combinación lineal de los demás vectores, existen $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_r$ tales que

$$\bar{v}_i = a_1\bar{v}_1 + \cdots + a_{i-1}\bar{v}_{i-1} + a_{i+1}\bar{v}_{i+1} + \cdots + a_r\bar{v}_r,$$

luego, tomando $a_i = -1$, tenemos que

$$a_1\bar{v}_1 + \cdots + a_r\bar{v}_r = \bar{0},$$

y $a_i \neq 0$, luego los vectores son linealmente dependientes. ■

[6] Observemos que "existe un i" no es formalizable en $\mathcal{L}_A^-$ mediante un particularizador, pues en C no pueden definirse los números naturales. No obstante, se formaliza como una disyunción $\bigvee_{i=1}^{r} \alpha_i$, donde α_i es la fórmula que afirma que $\bar{v}_i$ es combinación lineal de los vectores distintos de $\bar{v}_i$.

Teorema 1.11 (EV) *Si $\bar{v}_1, \ldots, \bar{v}_r$ son vectores linealmente independientes, al eliminar parte de ellos, los vectores que quedan son también linealmente independientes.*[7]

Demostración: Vamos a probar la implicación

$$\bar{v}_1, \bar{v}_2, \bar{v}_3 \text{ independientes} \rightarrow \bar{v}_1, \bar{v}_3 \text{ independientes}$$

de modo que quede claro que el argumento se puede adaptar para demostrar en C todas las fórmulas de la conclusión y para todos los casos particulares del esquema teoremático.[8]

Si $\bar{v}_1, \bar{v}_3$ son dependientes, existen escalares a_1, a_3 tales que $a_1\bar{v}_1 + a_3\bar{v}_3 = \bar{0}$ y $a_1 \neq 0 \vee a_3 \neq 0$, luego tomando $a_2 = 0$ resulta que $a_1\bar{v}_1 + a_2\bar{v}_2 + a_3\bar{v}_3 = \bar{0}$ y $a_1 \neq 0 \vee a_2 \neq 0 \vee a_3 \neq 0$. ■

Definición 1.12 (EV) Diremos que $\bar{v}_1, \ldots, \bar{v}_r$ son un *sistema generador* de una clase V (que necesariamente será una variedad lineal) si $V = \langle \bar{v}_1, \ldots, \bar{v}_r \rangle$. Si V tiene un sistema generador en este sentido, diremos que es una variedad lineal *finitamente generada.*

Ejemplo *Los vectores $\bar{e}_1, \ldots, \bar{e}_n$ son un sistema generador de k^n.*

En efecto, todo vector $\bar{v}$ puede expresarse como

$$\bar{v} = (v_1, \ldots, v_n) = v_1\bar{e}_1 + \cdots + v_n\bar{e}_n \in \langle \bar{e}_1, \ldots, \bar{e}_n \rangle,$$

luego $k^n = \langle \bar{e}_1, \ldots, \bar{e}_n \rangle$. ■

Teorema 1.13 (EV) *Si $V = \langle \bar{v}_1, \ldots, \bar{v}_r \rangle$ y $\bar{v} \in V$, $\bar{v} \neq \bar{0}$, entonces existe un índice i tal que $V = \langle \bar{v}_i, \ldots, \bar{v}_{i-1}, \bar{v}, \bar{v}_{i+1}, \ldots, \bar{v}_r \rangle$.*

Demostración: La hipótesis $\bar{v} \in V$ significa que existen $a_1, \ldots, a_r$ tales que $\bar{v} = a_1\bar{v}_1 + \cdots + a_r\bar{v}_r$. Como $\bar{v} \neq 0$, existe un i tal que $a_i \neq 0$. No perdemos generalidad si suponemos $a_r \neq 0$, pues en los otros casos se razona análogamente. Veamos que $V = \langle \bar{v}_1, \ldots, \bar{v}_{n-1}, \bar{v} \rangle$.

[7]Esto es un esquema teoremático que se formaliza mediante una conjunción. Por ejemplo, un caso particular es

$$\bar{v}_1, \bar{v}_2, \bar{v}_3 \text{ independientes} \rightarrow \bar{v}_1 \text{ independiente} \wedge \bar{v}_2 \text{ independiente} \wedge$$
$$\wedge \bar{v}_3 \text{ independiente} \wedge \bar{v}_1, \bar{v}_2 \text{ independientes } \wedge \bar{v}_1, \bar{v}_3 \text{ independientes} \wedge$$
$$\bar{v}^2, \bar{v}^3 \text{ independientes.}$$

[8]Tengamos presente que demostrar (constructivamente) un esquema teoremático significa dar un algoritmo que permita programar un ordenador para que genere una demostración de cualquier caso particular del esquema. Cualquier lector que entienda la demostración del caso particular que se muestra podría generar análogamente la demostración de cualquier otro caso particular y, si tiene conocimientos de programación, podría programar a un ordenador para que la generara automáticamente.

Si $\bar{w} \in V$, entonces existen $b_1, \ldots, b_n$ tales que $\bar{v} = b_1\bar{v}_1 + \cdots + b_n\bar{v}_n$, y sustituyendo en esta expresión $\bar{v}_r = -a_r^{-1}a_1\bar{v}_1 - \cdots - a_r^{-1}a_{r-1}\bar{v}_{r-1} + \bar{v}$ obtenemos una expresión de $\bar{w}$ como combinación lineal de $\bar{v}_1, \ldots, \bar{v}_{r-1}, \bar{w}$, luego $\bar{w} \in \langle \bar{v}_1, \ldots, \bar{v}_{r-1}, \bar{v} \rangle$. La inclusión opuesta se prueba de forma análoga. ■

En la prueba del teorema se ve que el índice i puede elegirse arbitrariamente entre los que correspondan a un coeficiente no nulo en una expresión de $\bar{v}$ como combinación lineal del generador de V.

Teorema 1.14 (EV) *Si $\bar{v}_1, \ldots, \bar{v}_r$ es un sistema generador de una variedad lineal V y $\bar{w}_1, \ldots, \bar{w}_s \in V$ forman un sistema libre, entonces*[9] $s \leq r$.

Demostración: Supongamos que $r < s$, que $\bar{v}_1, \ldots, \bar{v}_r$ es un generador de V y que $\bar{w}_1, \ldots, \bar{w}_s \in V$ es un sistema libre, y vamos a llegar a una contradicción.

Tenemos que $\bar{w}_1 \neq \bar{0}$, o de lo contrario no formaría parte de un sistema libre. Como $\bar{w}_1 \in V = \langle \bar{v}_1, \ldots, \bar{v}_r \rangle$, el teorema anterior nos da que existe un i (y no perdemos generalidad si suponemos que es $i = 1$, pues los demás casos se tratan análogamente) tal que $V = \langle \bar{w}_1, \bar{v}_2, \ldots, \bar{v}_r \rangle$.

Vamos a razonar inductivamente que (reordenando los vectores $\bar{v}_i$ si es preciso), se cumple que $V = \langle \bar{w}_1, \ldots, \bar{w}_i, \bar{v}_{i+1}, \ldots, \bar{v}_r \rangle$. Ya lo tenemos probado para $i = 1$. Si vale para $i < r$, entonces $\bar{w}_{i+1} \neq \bar{0}$ y $\bar{w}_{i+1} \in \langle \bar{w}_1, \ldots, \bar{w}_i, \bar{v}_{i+1}, \ldots, \bar{v}_r \rangle$, luego existen $a_1, \ldots, a_r$ tales que

$$\bar{w}_{i+1} = a_1\bar{w}_1 + \cdots + a_i\bar{w}_i + a_{i+1}\bar{v}_{i+1} + \cdots + a_r\bar{v}_r.$$

No puede ser $a_{i+1} = \cdots = a_r = 0$, porque entonces $\bar{w}_{i+1}$ sería combinación lineal de $\bar{w}_1, \ldots, \bar{w}_i$ y el sistema $\bar{w}_1, \ldots, \bar{w}_s$ sería ligado.

Ahora usamos que, por la observación tras el teorema anterior, podemos sustituir $\bar{w}_{i+1}$ por cualquier vector de $\bar{w}_1, \ldots, \bar{w}_i, \bar{v}_{i+1}, \ldots, \bar{v}_r$ cuyo coeficiente en la combinación lineal anterior no sea nulo, luego, concretamente, podemos tomar un cierto j entre $i + 1$ y n, y no perdemos generalidad si suponemos que es $i + 1$, con lo que $V = \langle \bar{w}_1, \ldots, \bar{w}_{i+1}, \bar{v}_{i+2}, \ldots, \bar{v}_r \rangle$.

De este modo, tras un número finito de pasos, obtenemos $V = \langle \bar{w}_1, \ldots, \bar{w}_r \rangle$, pero entonces llegamos a la contradicción de que $\bar{w}_{r+1}$ es combinación lineal de $\bar{w}_1, \ldots, \bar{w}_r$. ■

Definición 1.15 (EV) $\bar{v}^1, \ldots, v^n$ son una *base* de una variedad lineal V si son un sistema generador linealmente independiente. Por el teorema anterior, todas las bases de una variedad lineal V tienen el mismo número de elementos,[10] al que llamaremos *dimensión* de V y representaremos por $\dim V$.

La variedad lineal $0 = \{\bar{0}\}$ es finitamente generada, pero no tiene una base según la definición que hemos dado, pues su único sistema generador, el formado únicamente por $\bar{0}$, es linealmente dependiente. No obstante, es útil considerar por convenio que la clase vacía $\varnothing$ es una base de 0 (la única), y que, por consiguiente, $\dim 0 = 0$.

---

[9]Hay que entender esto como un esquema teoremático que, para cada $r < s$, afirma que si $\bar{w}_1, \ldots, \bar{w}_s \in \langle \bar{v}_1, \ldots, \bar{v}_r \rangle$, entonces $\bar{w}_1, \ldots, \bar{w}_s$ no forman un sistema libre.

[10]Esto es un esquema teoremático que, para cada $r \neq s$, afirma que si $V = \langle \bar{v}_1, \ldots, \bar{v}_r \rangle = \langle \bar{w}_1, \ldots, \bar{w}_s \rangle$, entonces $\bar{v}_1, \ldots, \bar{v}_r$ no es una base de V o bien $\bar{w}_1, \ldots, \bar{w}_s$ no es una base de V.

Hemos probado que $\bar{e}_1, \ldots, \bar{e}_n$ es una base de k^n, que recibe el nombre de *base canónica* de k^n, luego se cumple que $\dim k^n = n$.

Del teorema siguiente se desprende que toda variedad lineal finitamente generada tiene una base:

Teorema 1.16 (EV) *Si $V = \langle \bar{v}_1, \ldots, \bar{v}_r \rangle$ y $v_r \in \langle \bar{v}_1, \ldots, \bar{v}_{r-1} \rangle$, entonces también $V = \langle \bar{v}_1, \ldots, \bar{v}_{r-1} \rangle$.*

Demostración: Las dos inclusiones opuestas se siguen del teorema 1.8. ■

Así, si $V = \langle \bar{v}_1, \ldots, \bar{v}_r \rangle$ es una variedad finitamente generada (descartando el caso trivial en que $V = 0$) si el sistema generador dado no es linealmente independiente, es que uno de sus vectores es combinación lineal de los demás, luego aplicando el teorema anterior puede eliminarse, y tras un número finito de pasos tenemos que llegar a una base.

Teorema 1.17 (EV) *Si V es una variedad lineal finitamente generada de dimensión d y $\bar{v}_1, \ldots, \bar{v}_r \in V$ son vectores linealmente independientes, con $r < d$, entonces existen $\bar{v}_{r+1}, \ldots, \bar{v}_d \in V$ tales que $\bar{v}_1, \ldots, \bar{v}_d$ son una base de V.*

Demostración: Tenemos que $\langle \bar{v}_1, \ldots, \bar{v}_r \rangle < V$, pues los vectores no pueden generar V, ya que entonces serían una base y tendría que haber d vectores. Por lo tanto, existe un $\bar{v}_{r+1} \in V \setminus \langle \bar{v}_1, \ldots, \bar{v}_r \rangle$, y entonces $\bar{v}_1, \ldots, \bar{v}_{r+1} \in V$ son linealmente independientes.

En efecto, si $a_1\bar{v}_1 + \cdots + a_{r+1}\bar{v}_{r+1} = \bar{0}$, si $a_{r+1} \neq 0$, entonces podemos despejar $\bar{v}_{r+1}$ y llegamos a que $\bar{v}_{r+1} \in \langle \bar{v}_1, \ldots, \bar{v}_r \rangle$, contradicción. Por lo tanto, tiene que ser $a_{r+1} = 0$ y, como $\bar{v}_1, \ldots, \bar{v}_r$ son linealmente independientes, los demás escalares también son nulos.

Si $r + 1 < d$ podemos repetir el proceso, y tras un número finito de pasos llegamos a unos vectores $\bar{v}_1, \ldots, \bar{v}_d \in V$ linealmente independientes. Dichos vectores tienen que ser una base de V, pues en caso contrario, podríamos repetir el proceso una vez más para obtener un sistema libre con $d + 1$ vectores, en contradicción con el teorema 1.14. ■

Teorema 1.18 (EV) *Si V es una variedad lineal finitamente generada y $W \leq V$ es una subvariedad lineal, entonces W también es finitamente generada,* $\dim W \leq \dim V$ *y* $\dim W = \dim V$ *si y sólo si $W = V$.*

Demostración: Sea $\dim V = d$. Si $W = 0$ la conclusión es trivial. En caso contrario existe $\bar{w}_1 \in W$ no nulo, que es un vector linealmente independiente. Si $\langle \bar{w}_1 \rangle < W$, entonces existe un $\bar{w}_2 \in W \setminus \langle \bar{w}_1 \rangle$, el mismo argumento empleado en la prueba del teorema anterior muestra que $\bar{w}_1, \bar{w}_2 \in W$ son vectores linealmente independientes, pero al cabo de a lo sumo d pasos tenemos que llegar a que $W = \langle \bar{w}_1, \ldots, \bar{w}_r \rangle$, con $r \leq d$, pues en caso contrario habríamos construido un sistema libre de $d + 1$ vectores en V.

Si $r < d$, entonces $W < V$, pues de lo contrario tendríamos una base de V con d vectores. Si $r = d$ entonces $W = V$, pues en caso contrario podríamos encontrar en V un nuevo vector que al añadirlo a $\bar{w}_1, \ldots, \bar{w}_d$ formaría un sistema libre con $d + 1$ vectores, lo cual es imposible. ■

Así, como k^n es una variedad finitamente generada, todas las variedades lineales formadas por los vectores que estamos considerando (que son subvariedades de k^n) son finitamente generadas, pero esto no es una consecuencia de los axiomas de espacio vectorial.

Teorema 1.19 *Si $\bar{v}^1, \ldots, \bar{v}^n$ son una base de una variedad lineal V, entonces*

$$\bigwedge \bar{v} \in V \overset{1}{\bigvee} a_1 \cdots a_n \ \bar{v} = a_1\bar{v}^1 + \cdots + a_n\bar{v}_n.$$

Demostración: La existencia se tiene por definición de sistema generador, y si

$$a_1\bar{v}^1 + \cdots + a_n\bar{v}_n = \bar{v} = b_1\bar{v}^1 + \cdots + b_n\bar{v}_n,$$

entonces

$$(a_1 - b_1)\bar{v}_1 + \cdots + (a_n - b_n)\bar{v}_n = \bar{0},$$

luego por definición de independencia lineal $a_1 = b_1 \wedge \cdots \wedge a_n = b_n$. ■

Definición 1.20 (EV) Si $\bar{v}_1, \ldots, \bar{v}_r$ es una base de una variedad lineal V, los únicos escalares $a_1, \ldots, a_r$ dados por el teorema anterior se llaman *coordenadas* del vector $\bar{v}$ en dicha base.

Teorema 1.21 (EV) *Si V y W son variedades lineales, también lo son $V \cap W$ y*

$$V + W = \{\bar{x} \mid \bigvee \bar{v}\bar{w}(\bar{x} = \bar{v} + \bar{w} \wedge \bar{v} \in V \wedge \bar{w} \in W)\}.$$

Si V y W son finitamente generadas, también lo son $V \cap W$ y $V + W$, y entonces

$$\dim(V + W) = \dim V + \dim W - \dim(V \cap W).$$

Demostración: La prueba de que $V \cap W$ y $V + W$ son variedades lineales no ofrece ninguna dificultad. Claramente $V \cap W$ es finitamente generada. Sea $\bar{x}_1, \ldots, \bar{x}_d$ una base de $V \cap W$. Podemos completarla hasta una base $\bar{x}_1, \ldots, \bar{x}_d, \bar{v}_{d+1}, \ldots, \bar{v}_r$ de V y hasta otra base $\bar{x}_1, \ldots, \bar{x}_d, \bar{w}_{d+1}, \ldots, \bar{w}_s$ de W. Basta probar que $\bar{x}_1, \ldots, \bar{x}_d, \bar{v}_{d+1}, \ldots, \bar{v}_r, \bar{w}_{d+1}, \ldots, \bar{w}_s$ es una base de $V + W$, pues entonces

$$\dim(V + W) = d + r - d + s - d = r + s - d = \dim V + \dim W - \dim(V \cap W).$$

Todo vector de $V + W$ es la suma de una combinación lineal de los vectores $\bar{x}_1, \ldots, \bar{x}_d, \bar{v}_{d+1}, \ldots, \bar{v}_r$ y otra de $\bar{x}_1, \ldots, \bar{x}_d, \bar{w}_{d+1}, \ldots, \bar{w}_s$, y es claro que la suma se reduce a una combinación lineal de $\bar{x}_1, \ldots, \bar{x}_d, \bar{v}_{d+1}, \ldots, \bar{v}_r, \bar{w}_{d+1}, \ldots, \bar{w}_s$, luego estos vectores forman un sistema generador, y esto ya prueba que la suma es finitamente generada. Supongamos ahora que

$$a_1\bar{x}_1 + \ldots + a_d\bar{x}_d + b_{d+1}\bar{v}_{d+1} + \ldots + b_r\bar{v}_r + c_{d+1}\bar{w}_{d+1} + \ldots + c_s\bar{w}_s = \bar{0}.$$

Entonces

$$a_1\bar{x}_1 + \ldots + a_d\bar{x}_d + b_{d+1}\bar{v}_{d+1} + \ldots + b_r\bar{v}_r = -c_{d+1}\bar{w}_{d+1} - \ldots - c_s\bar{w}_s,$$

el miembro izquierdo está en V y el miembro derecho está en W, luego ambos están en $V \cap W$. Ahora bien, cada vector de $V \cap W$ admite una expresión como combinación lineal de $\bar{x}_1, \ldots, x_d$, que es también una expresión como combinación lineal de la base $\bar{x}_1, \ldots, \bar{x}_d, \bar{v}_{d+1}, \ldots, \bar{v}_r$ cuyas últimas coordenadas son nulas. Por la unicidad de las coordenadas, concluimos que todos los vectores de $V \cap W$ tienen nulas sus últimas coordenadas respecto de la base de V considerada, lo que en nuestro caso se traduce en que $b_{d+1} = \cdots = b_r = 0$. Por simetría podemos concluir igualmente que $c_{d+1} = \cdots = c_s = 0$, y entonces tenemos que

$$a_1\bar{x}_1 + \ldots + a_d\bar{x}_d = 0,$$

luego también $a_1 = \cdots a_d = 0$. ■

1.4 Polinomios

En la sección anterior hemos estudiado vectores con un número fijo de n componentes. Ahora vamos a considerar vectores consistentes en sucesiones finitas de números de longitud arbitraria, pero con el convenio de que la prolongación con ceros de una sucesión la consideraremos como “la misma sucesión”.

Empezamos introduciendo los convenios de notación oportunos que faciliten trabajar con estos nuevos vectores. En primer lugar, en esta sección adoptamos el criterio de que la notación $\bar{v}_n$ se refiera a bloques de $n+1$ variables $\bar{v}_n = (v_0, \ldots, v_n)$ en lugar de a bloques de n variables, como hasta ahora. La identificación de las sucesiones que se obtienen prolongando con ceros se plasma en la definición siguiente (válida para todos los naturales $m \leq n$):

$$\bar{v}_m = \bar{v}_n \equiv \bar{v}_n = \bar{v}_m \equiv v_1 = w_1 \land \cdots \land v_m = w_m \land w_{m+1} = 0 \land \cdots \land w_n = 0.$$

La suma de vectores se define ahora, para $m \leq n$, como

$$\bar{v}_m + \bar{w}_n \equiv \bar{w}_n + \bar{v}_m = (v_1 + w_1, \ldots, v_m + w_m, w_{m+1}, \ldots, w_n),$$

y observamos que esta suma es compatible con la igualdad que hemos definido, en el sentido de que si $\bar{v}_m = \bar{v}'_{m'}$ y $\bar{w}_n = \bar{w}'_{n'}$ entonces $\bar{v}_m + \bar{w}_n = \bar{v}'_{m'} + \bar{w}'_{n'}$.

El vector nulo lo representaremos ahora como $0^* = (0)$. Definimos también

$$-\bar{v}_n = (-v_0, \ldots, -v_n), \qquad a(a_0, \ldots, a_n) = (aa_0, \ldots, aa_n).$$

Con estas definiciones se demuestra también sin dificultad el teorema 1.4, es decir, que los vectores de longitud variable cumplen también los axiomas de espacio vectorial y, por consiguiente, todos los teoremas que hemos demostrado a partir de ellos.

La novedad es que ahora definimos un producto de vectores: $\bar{v}_m \cdot \bar{w}_n = \bar{x}_{m+n}$, donde[11]

$$x_k = \sum_{i+j=k} v_i w_j.$$

Esto es un esquema de definición que tiene una versión particular para cada valor de m y n. Por ejemplo, para $m = 2$ y $n = 1$ sería

$$(v_0, v_1, v_2)(w_0, w_1) = (v_0 w_0, v_0 w_1 + v_1 w_0, v_0 w_2 + v_1 w_1 + v_2 w_0).$$

Observamos también que, al igual que la suma, este producto es compatible con la igualdad de vectores.

De este modo, los números son también vectores (sucesiones de longitud 0), y si particularizamos la definición de producto al caso de un vector de longitud 0 por otro de longitud n, obtenemos:

$$a(a_0, \ldots, a_n) = (aa_0, \ldots, aa_n),$$

que es el producto por escalares que ya habíamos definido, luego el producto de vectores extiende al producto por escalares.

Veamos ahora las propiedades del producto que acabamos de definir:

Teorema 1.22 *Se cumple:*

1. $(\bar{p} + \bar{q}) + \bar{r} = \bar{p} + (\bar{q} + \bar{r})$,
2. $\bar{p} + \bar{q} = \bar{q} + \bar{p}$,
3. $\bar{p} + 0 = \bar{p}$,
4. $\bar{p} + (-\bar{p}) = 0$,
5. $(\bar{p}\bar{q})\bar{r} = \bar{p}(\bar{q}\bar{r})$,
6. $\bar{p}\bar{q} = \bar{q}\bar{p}$,
7. $\bar{p} \cdot 1 = \bar{p}$;
8. $\bar{p}(\bar{q} + \bar{r}) = \bar{p}\bar{q} + \bar{p}\bar{r}$,
9. $1 \neq 0$,
10. $\bar{p}\bar{q} = 0 \rightarrow \bar{p} = 0 \lor \bar{q} = 0$.

[11]He aquí otro ejemplo de sumatorio en el que no nos molestamos en especificar el orden de los sumandos.

Nota No indicamos las longitudes de las sucesiones porque estas propiedades se cumplen cualesquiera que sean éstas.[12]

DEMOSTRACIÓN: Las cuatro primeras propiedades son las mismas que ya conocemos para vectores.

5. El término n-simo de $(\bar{p}\bar{q})\bar{r}$ es

$$\sum_{h+k=n} (\bar{p}\bar{q})_h r_j = \sum_{h+k=n} \sum_{i+j=h} p_i q_j r_k = \sum_{i+j+k=n} p_i q_j r_k,$$

y si calculamos el término n-simo de $\bar{p}(\bar{q}\bar{r})$ llegamos a la misma expresión.

Las propiedades 6. y 8. se prueban análogamente, 7. es una de las propiedades de los vectores y 9. es trivial.

Para probar 10. suponemos que $\bar{p}_m \neq 0 \wedge \bar{q}_n \neq 0$. No perdemos generalidad[13] si suponemos que $p_m \neq 0 \neq q_n$, y entonces es fácil ver que el término mn-ésimo de $\bar{p}_m\bar{q}_n$ es $p_m q_n \neq 0$, luego $\bar{p}_m\bar{q}_n \neq 0$. ■

Las propiedades de este teorema son precisamente los axiomas de C salvo que falta la existencia de inverso y, a cambio, tenemos la última propiedad, que en los cuerpos se demuestra precisamente a partir de dicha existencia. No obstante, muchos de los resultados básicos de la sección 1.2 no dependen de la existencia de inversos y son válidos también en este contexto. Por ejemplo, podemos trabajar normalmente con sumas y productos finitos, están definidas las potencias de exponente no negativo, etc.

El vector $X = (0, 1)$ recibe el nombre de *indeterminada*, y una simple inducción demuestra que $X^n = (0, \ldots, 0, 1)$, con el 1 en la posición n-sima (empezando por la 0-ésima). Por consiguiente, todo vector $\bar{p}_n$ puede expresarse como

$$\bar{p} = (p_0, \ldots, p_n) = \sum_{i=0}^{n} p_i X^i = p_0 + p_1 X + \cdots + p_n X^n.$$

En lo sucesivo usaremos la notación $p^n(X)$ en lugar de $\bar{p}_n$ para indicar que la letra p no representa una variable, sino un bloque de $n+1$ variables. Cuando el valor de n sea irrelevante lo omitiremos.

A estos vectores que estamos considerando, con la suma y el producto que hemos definido, los llamaremos *polinomios.*

En estos términos, las operaciones con polinomios se expresan así:

$$p^n(X) + q^n(X) = \sum_{i=0}^{n} (p_i + q_i) X^i, \qquad p^m(X) q^n(X) = \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} p_i q_j \Big) X^k.$$

[12]Como en el teorema 1.4, cada propiedad es en realidad un esquema teoremático, que se concreta en un teorema distinto para cada combinación de longitudes de los vectores que intervienen. Por ejemplo, el caso concreto de la propiedad 6. correspondiente a $\bar{p}_2$ y $\bar{q}_1$, sería

$$p_0 q_0 = q_0 p_0 \wedge p_0 q_1 + p_1 q_0 = q_1 p_0 + q_0 p_1 \wedge p_2 q_0 + p_1 q_1 = q_0 p_2 + q_1 p_1 \wedge p_2 q_1 = q_1 p_2.$$

[13]Este paso no es trivial, pero será más claro si lo analizamos más adelante, al discutir la prueba del teorema 1.23.

Si $\bar{p}_n$ es un bloque de variables, $p^n(X)$ no es sino una forma alternativa de denotarlo. Si queremos hacer explícitas las n variables que aparecen en él, por ejemplo, para especificar sustituciones, escribiremos

$$p^n(X) \equiv p(p_0, \ldots, p_n; X) \equiv (p_0, \ldots, p_n),$$

de modo que $p^n(t_0, \ldots, t_n; X)$ será una forma alternativa de representar el multitérmino $(t_0, \ldots, t_n)$.

La indeterminada X no es una variable, sino el bloque de constantes $(0, 1)$, por lo que en principio no tiene sentido sustituirla por términos, pero eso no quita para que a cada polinomio $p^n(X)$ le podamos asociar el término

$$p^n(x) \equiv p_0 + p_1 x + \cdots + p_n x^n,$$

donde x es una variable de $\mathcal{L}_A^-$ distinta de las que aparecen en $\bar{p}$, de modo que si $\bar{p}$ es un bloque de $n+1$ variables entonces $p(x)$ es un término de $\mathcal{L}_A^-$ con $n+2$ variables libres, lo que nos permite sustituirlas todas para formar términos $p(t_0, \ldots, t_n; t)$, o simplemente $p(t)$ cuando los coeficientes del polinomio sean conocidos o irrelevantes. Así pues, en la práctica podemos sustituir la indeterminada X por cualquier término, y esta sustitución es consistente con la suma y el producto de términos en el sentido siguiente:

$$(p+q)(x) = p(x) + q(x), \qquad (pq)(x) = p(x)q(x).$$

Por ejemplo, en el caso del producto esto significa que, aunque los dos miembros de

$$\sum_{k=0}^{m+n} \Big(\sum_{i+j=k} p_i q_j \Big) x^k = \Big(\sum_{i=1}^{m} p_i x^i \Big) \Big(\sum_{j=1}^{n} q_j x^j \Big),$$

no son el mismo mutitérmino de $\mathcal{L}_A^-$, en C se demuestra que son iguales, simplemente desarrollando el miembro derecho usando las propiedades de la suma y el producto de C. Lo mismo vale para la suma de polinomios.

Teorema 1.23 *Si $p^n(X) \neq 0$, existe*[14] *un único número natural $d \leq n$ y un único $\bar{q} \in k^d$ tal que $p^n(X) = q^d(X)$ y $q_d \neq 0$.*

Al valor de d dado por el teorema anterior lo llamaremos *grado* del polinomio $p_n(X)$. Equivalentemente:

$$\operatorname{grad} p^n(X) = d \equiv p_d \neq 0 \land p_{d+1} = 0 \land \cdots \land p_n = 0.$$

Convendremos en que el polinomio nulo tiene grado 0.

[14]Este teorema es trivial, pero lo enunciamos para discutir su formalización en C. Por ejemplo, para $n = 2$ se trata de la fórmula siguiente:

$$a + bX + cX^2 \neq 0 \to c \neq 0 \land (a + bX + cX^2 = a + bX + cX^2) \lor$$
$$(b \neq 0 \land a + bX + cX^2 = a + bX) \lor (a \neq 0 \land a + bX + cX^2 = a).$$

La unicidad es la conjunción de las negaciones de cada par de conjunciones de dos términos cualesquiera de la disyunción.

Así, cada vez que en una demostración tenemos un polinomio $p^n(X)$ y decimos: "podemos suponer que $p_n \neq 0$", técnicamente estamos desdoblando la demostración en $n+1$ casos totalmente análogos correspondientes a la disyunción precedente, casos que habitualmente podrán tratarse al mismo tiempo de forma esquemática, en términos de un d arbitrario.

Si $p(X)$ es un polinomio no nulo de grado n, el coeficiente p_n se llama *coeficiente director* de $p(X)$. El polinomio es *mónico* si $p_n = 1$.

Es claro que si $p(X)$ es un polinomio no nulo de grado n, podemos expresarlo como $p(X) = p_n\, q(X)$, donde $q(X)$ es un polinomio mónico de grado n. Basta definir $q_i = p_n^{-1} p_i$.

Si $\bar{p}_{n-1} = (p_0, \ldots, p_{n-1})$ es un bloque de n variables, usaremos la notación

$$p_1^n(X) = p_0 + p_1 X + \cdots + p_{n-1} X^{n-1} + X^n$$

para representar polinomios mónicos.

De las definiciones de la suma y el producto se sigue fácilmente que

$$\operatorname{grad}(p(X) + q(X)) \leq \text{máx}\{\operatorname{grad} p(X), \operatorname{grad} q(X)\},$$

$$p(X) \neq 0 \neq q(X) \to \operatorname{grad}(p(X)q(X)) = \operatorname{grad} p(X) + \operatorname{grad} q(X).$$

División euclídea y raíces Vamos a demostrar que es posible efectuar divisiones euclídeas entre polinomios, de lo cual extraeremos numerosas consecuencias.

Teorema 1.24 *Dados polinomios $p(X)$, $q(X)$, el segundo no nulo, existen unos únicos polinomios $c(X)$ y $r(X)$ tales que*

$$p(X) = q(X)c(X) + r(X), \qquad (r(X) = 0 \vee \operatorname{grad} r(X) < \operatorname{grad} q(X)).$$

Demostración: Supongamos la existencia de cociente y resto cuando $p(X)$ tiene grado $< m$ y que $p(X)$ tiene grado m. Si $\operatorname{grad} p(X) < \operatorname{grad} q(X)$, basta tomar como $c(X)$ el polinomio nulo y $r(x) = p(X)$. En caso contrario, si $n = \operatorname{grad} q(X)$, el polinomio $p'(X) = p(X) - p_m q_n^{-1} X^{m-n} q(X)$ tiene grado $< m$, luego por hipótesis de inducción

$$p(X) - p_m q_n^{-1} X^{m-n} q(X) = q(X)c'(X) + r(X), \qquad \operatorname{grad} r(X) < \operatorname{grad} q(X).$$

Por lo tanto, la descomposición

$$p(X) = q(X)(p_m q_n^{-1} X^{m-n} + c'(X)) + r(X)$$

cumple lo requerido.

Veamos ahora la unicidad. Suponemos que

$$p(X) = q(X)c(X) + r(X) \wedge \operatorname{grad} r(X) < \operatorname{grad} q(X)$$

y

$$p(X) = q(X)c'(X) + r'(X) \wedge \operatorname{grad} r'(X) < \operatorname{grad} q(X),$$

con lo que $q(X)(c(X) - c'(X)) = r'(X) - r(X)$.

Si $c(X) - c'(X) \neq 0$, el grado del miembro izquierdo es $\geq \operatorname{grad} q(X)$, mientras que el grado del miembro derecho es $< \operatorname{grad} q(X)$, lo cual es una contradicción. Por lo tanto $c(X) = c'(X)$, con lo que el miembro izquierdo es nulo, el derecho también, y los restos también son iguales. ■

Nota El lector debería reflexionar hasta convencerse de que el cociente y el resto construidos por el procedimiento inductivo considerado en la prueba del teorema anterior no son sino los que se obtienen al aplicar el conocido algoritmo de la división euclídea. En realidad, no es necesario preocuparse por adaptar la demostración en C al esquema de la inducción, sino que, dado que se trata de un esquema teoremático con un caso particular distinto para cada $p^m(X)$ y cada $q^n(X)$, podemos limitarnos a calcular en cada caso la división euclídea correspondiente y constatar en C que el cociente y el resto obtenidos cumplen lo requerido.

Por simplificar vamos a suponer que el divisor es mónico, y así partimos de dos expresiones $p^m(X)$ y $q_1^n(X)$, en las que $\bar{p}_m$ y $\bar{q}_{n-1}$ son bloques de variables de $\mathcal{L}_A^-$. Con papel y lápiz (es decir, sin tener en cuenta C ni $\mathcal{L}_A^-$ para nada), podemos realizar la división euclídea de dichos polinomios. Por ejemplo, para $m = 3$ y $n = 1$ es

$$
\begin{array}{llll|l}
p_3X^3 & +\ p_2X^2 & +p_1X & +p_0 & x-q_0 \\ \cline{5-5}
\underline{p_3X^3} & \underline{-\,p_3q_0x^2} & & & p_3X^2+(p_2+p_3q_0)X+(p_1+p_2q_0+p_3q_0^2) \\
 & (p_2+p_3q_0)X^2 & +p_1X & & \\
 & \underline{(p_2+p_3q_0)X^2} & \underline{-q_0(p_2+p_3q_0)X} & & \\
 & & (p_1+p_2q_0+p_3q_0^2)X & +p_0 & \\
 & & \underline{(p_1+p_2q_0+p_3q_0^2)X} & \underline{-q_0(p_1+p_2q_0+p_3q_0^2)} & \\
 & & & p_0+p_1q_0+p_2q_0^2+p_3q_0^3 &
\end{array}
$$

En general, de este modo podemos calcular unos términos $c^i_{m,n}(\bar{p}_m, \bar{q}_{n-1})$, $r^i_{m,n}(\bar{p}_m, \bar{q}_{n-1})$, de modo que llamando

$$c_{m,n}(\bar{p}_m, \bar{q}_{n-1}; X) \equiv h(c^0_{m,n}, \ldots, c^{m-n}_{m,n}; X),$$

$$r_{m,n}(\bar{p}_m, \bar{q}_{n-1}; X) \equiv h(r^0_{m,n}, \ldots, r^{n-1}_{m,n}; X),$$

se cumple que

$$\vdash_{\mathrm{C}} p^m(X) = q_1^n(X)c_{m,n}(X) + r_{m,n}(X).$$

En el ejemplo indicado, estos términos son

$$c^0_{3,1} = p_1 + p_2q_0 + p_3q_0^2, \qquad c^1_{3,1} = p_2 + p_3q_0, \qquad c^2_{3,1} = p_3,$$

$$r^0_{3,1} = p_0 + p_1q_0 + p_2q_0^2 + p_3q_0^3.$$

La demostración en C de $p^m(X) = q_1^n(X)c_{m,n}(X) + r_{m,n}(X)$ se reduce a operar el miembro derecho y constatar que el resultado es el miembro izquierdo, y eso prueba el teorema (por lo menos la parte de existencia para divisor mónico), pues no hay ningún "para todo polinomio" que formalizar en C, sino que se trata demostrar que existe una prueba particular para cada valor posible de m y n y eso es lo que hacemos al constatar que hay un algoritmo de división que general un cociente y un resto que cumplen lo requerido y que la comprobación de que cumplen lo requerido es formalizable en C.

Hemos exigido que el divisor sea mónico para que el cociente y el resto no tengan fracciones y sean términos de $\mathcal{L}_A^-$ sin conceptos definidos, pero el caso general se reduce a éste expresando $q(X) = q_n q_1'^n(X)$. ■

Veamos las consecuencias de la división euclídea:

Definición 1.25 Una *raíz* de un polinomio $p(X)$ es cualquier número que cumpla $p(d) = 0$.

Cada raíz de un polinomio se corresponde con un factor de grado 1:

Teorema 1.26 $p^n(d) = 0 \to p^n(X) = c_{n,1}(X)(X - d)$.

Demostración: En general, tenemos que $p^n(X) = c_{n,1}(X)(X - d) + r_{n,1}$, pero al evaluar $X = d$ queda que $r_{n,1} = 0$. ■

Más precisamente:

Teorema 1.27 *Si $p(X)$ es un polinomio no nulo de grado n, existe*[15] *un $m \leq n$ y un polinomio mónico $q(X)$ de modo que*

$$p(X) = p_n\ (X - d)^m q(X) \land q(d) \neq 0.$$

Demostración: Razonamos por inducción sobre n. Si $n = 0$ basta tomar $m = 0$. Supongamos que el resultado es cierto para n y consideremos un polinomio $p^{n+1}(X) = p_{n+1} q_1^{n+1}(X)$.

Si $q_1^{n+1}(d) \neq 0$, entonces se cumple el teorema con $m = 0$. Si no es así, podemos aplicar el teorema anterior, que nos da unos $\bar{p}'_{n-1}$ tales que

$$p^{n+1}(X) = p_{n+1}\ (X - d)\, p_1'^n(X) = p_{n+1}(X - d)^{m+1}\ q_1^{n+1-(m+1)}(X),$$

con $q_1^{n+1-(m+1)}(d) \neq 0$, donde hemos aplicado la hipótesis de inducción. ■

Aplicando repetidamente el teorema anterior obtenemos:

Teorema 1.28 *Todo polinomio no nulo $p(X)$ de grado n se descompone en la forma*

$$p(X) = p_n(X - d_1)^{m_1} \cdots (X - d_r)^{m_r} q(X),$$

donde los números d_i son distintos dos a dos y $q(X)$ es un polinomio mónico sin raíces.

Observemos que los números d_i son precisamente las raíces de $p(X)$, de modo que

$$p(d_1) = \cdots = p(d_r) = 0 \land \bigwedge x(p(x) = 0 \to x = d_1 \lor \cdots \lor x = d_r).$$

Como consecuencia en $\mathrm{C}_{\mathrm{inf}}$ (es decir, la teoría C más el esquema axiomático de infinitud) se puede probar que la evaluación de un polinomio determina el polinomio:

[15] Para formalizar este teorema hay que plantear un esquema teoremático que, para cada natural n, considere un $p^n(X)$. La existencia de m se plantea como una disyunción $\bigvee_{m \leq n} \alpha_m$, donde α_m plantea la existencia de $\bar{q}^{n-m}$ tales que $q_1^{n-m}(X)$ cumple lo requerido.

Teorema 1.29 ($C_{\mathbf{inf}}$) $p(X) = q(X) \leftrightarrow \bigwedge x\, p(x) = q(x)$.

Llamando $f(X) = p(X) - q(X)$ el teorema es equivalente a probar que $\bigwedge x\, f(x) = 0 \to f(X) = 0$. Si $f(X) \neq 0$ tiene grado n, la observación precedente nos da $d_1, \ldots, d_r$ tales que

$$\bigwedge x(f(x) = 0 \to x = d_1 \vee \cdots \vee x = d_r).$$

Por lo tanto, tenemos $\bigwedge x(x = d_1 \vee \cdots \vee x = d_r)$, pero esto contradice al axioma $r + 1$-ésimo del esquema de infinitud. ■

Divisibilidad Para cada par de naturales m y n, definimos la fórmula[16]

$$p_m(X) \mid q_n(X) \equiv \bigvee \bar{c}_n\ q_n(X) = p_m(X)c_n(X).$$

Menos técnicamente, un polinomio $p(X)$ divide a otro $q(X)$ si existe un tercer polinomio $c(X)$ tal que $q(X) = p(X)c(X)$. Los hechos siguientes se prueban sin dificultad:

1. $a \neq 0 \to a \mid q(X)$,
2. $p(X) \mid q(X) \wedge q(X) \mid p(X) \leftrightarrow \bigvee a\ (a \neq 0 \wedge p(X) = a\, q(X))$,
3. $p(X) \mid q(X) \wedge q(X) \mid r(X) \to p(X) \mid r(X)$,
4. $p(X) \mid q(X) \wedge p(X) \mid r(X) \to p(X) \mid q(X) + r(X)$.

Diremos que dos polinomios $p(X)$ y $q(X)$ son *asociados* si se dividen mutuamente, lo cual, según la propiedad 2., equivale a que se diferencien en un factor constante no nulo. En particular, cada polinomio es asociado a un único polinomio mónico. Por ello, en cuestiones relacionadas con la divisibilidad, nunca perdemos generalidad si nos limitamos a considerar polinomios mónicos.

El teorema siguiente prueba la existencia del máximo común divisor de dos polinomios, junto al hecho de que puede expresarse como combinación lineal de dichos polinomios:

Teorema 1.30 *Dados dos polinomios $p(X)$ y $q(X)$, existen polinomios*[17] *$d(X)$, $u(X)$ y $v(X)$ tales que*

$$d(X) \mid p(X) \wedge d(X) \mid q(X) \wedge d(X) = u(X)p(X) + v(X)q(X).$$

[16] Notemos que el cuantificador requiere concretar el número de variables que consideramos, y ponemos n porque el grado de $q_n(X)$ es a lo sumo n, luego n es también el máximo grado posible del cociente.

[17] Como siempre, desde un punto de vista técnico tenemos un esquema teoremático, con un caso concreto para cada par de naturales m y n, que parte de polinomios $p^m(X)$, $q^n(X)$ y afirma la existencia de naturales r, s, t (es decir, una disyunción con un número finito de fórmulas $\alpha_{r,s,t}$) y de multivariables $\bar{u}, \bar{v}, \bar{d}$ de forma que $d_1^t(X)$, $u^r(X)$ y $v^s(X)$ cumplen lo pedido.

Demostración: Si $p(X) = p^m(X)$ y $q(X) = q^n(X)$, razonamos por inducción sobre $m + n$. Si $m + n = 0$ es porque $m = n = 0$, si $p = q = 0$, entonces tomamos $d = u = v = 0$, mientras que si, por ejemplo, $p \neq 0$, tomamos $d = 1$, $u = 1/p$, $v = 0$.

Supongamos que el teorema vale cuando la suma de los grados es menor que $m + n$. Pongamos que $m \leq n$ y dividamos

$$q^n(X) = p^m(X)c(X) + r^{m-1}(X),$$

Si $r(X) = 0$ es que $p^m(X) \mid q^n(X)$, y entonces basta tomar $d(X) = p(X)$, $u = 1$, $v = 0$.

En caso contrario podemos aplicar la hipótesis de inducción a $r^{m-1}(X)$ y $p^m(X)$, lo que nos da unos polinomios

$$d(X) \mid r^{m-1}(X) \wedge d(X) \mid p^m(X) \wedge d(X) = u(X)r^{m-1}(X) + v(X)p^m(X).$$

Es claro entonces que $d(X) \mid q^n(X)$. Más aún,

$$d(X) = u(X)(q^n(X) - p^m(X)c(X)) + v(X)p^m(X) =$$

$$(v(X) - u(X)c(X))\ p^m(X) + u(X)\ q^n(X).$$

Basta tomar $u'(X) = v(X) - u(X)c(X)$, $v'(X) = u(X)$. ■

Definición 1.31 Para cada número natural $n \geq 1$, diremos que el polinomio $p^n(X)$ *es irreducible* si $\operatorname{grad} p(X) \geq 1$ y sus únicos divisores son los constantes y sus asociados, es decir:

$$\bigwedge \bar{q}_n (q^n(X) \mid p^n(X) \to \operatorname{grad} q^n(X) = 0 \vee \operatorname{grad} q^n(X) = \operatorname{grad} p^n(X)).$$

Notemos que si un polinomio divide a otro del mismo grado, el cociente tiene que tener grado 0, es decir, es constante, luego ambos polinomios son asociados.

Trivialmente, todo polinomio $X - a$ es irreducible. Por el teorema 1.26, un polinomio irreducible de grado mayor que 1 no puede tener raíces.

Cuando aplicamos el teorema anterior a un polinomio irreducible obtenemos lo siguiente:

Teorema 1.32 *Si $p(X)$ es irreducible, o bien $p(X) \mid q(X)$ o bien existen polinomios $u(X)$, $v(X)$ tales que $u(X)p(X) + v(X)q(X) = 1$.*

Demostración: Con la notación del teorema anterior, $d(X) \mid p(X)$, pero por la irreducibilidad de $p(X)$, o bien $d = 1$ o bien $p(X)$ es asociado a $d(X)$. En el segundo caso $p(X) \mid d(X) \mid q(X)$, mientras que si $d = 1$ se cumple la segunda posibilidad que indica el enunciado. ■

Como consecuencia, a su vez:

Teorema 1.33 *Si $r(X)$ es irreducible y $r(X) \mid p(X)q(X)$, entonces $r(X) \mid p(X)$ o $r(X) \mid q(X)$.*

DEMOSTRACIÓN: Si no $r(X) \mid p(X)$, por el teorema anterior tenemos que

$$u(X)r(X) + v(X)p(X) = 1,$$

luego

$$u(X)r(X)q(X) + v(X)p(X)q(X) = q(X),$$

y como $r(X) \mid p(X)q(X)$, concluimos que $r(X) \mid q(X)$. ■

Teorema 1.34 *Todo polinomio no constante tiene un factor irreducible.*

DEMOSTRACIÓN: Partimos de $p^n(X)$ con $n \geq 1$ y razonamos por inducción sobre n. Si $p^1(X)$ tiene grado 1, entonces es irreducible y la conclusión es trivial. Supuesto cierto para n, si $p^{n+1}(X)$ es irreducible la conclusión es trivial. En caso contrario existe un polinomio $q_1^m(X) \mid p^{n+1}(X)$ con $1 < m < n+1$. Por hipótesis de inducción $q_1^m(X)$ tiene un factor irreducible, que también lo será de $p^{n+1}(X)$. ■

Teorema 1.35 *Todo polinomio $p(X)$ no constante se descompone en producto*[18] *de polinomios irreducibles $p(X) = p_1(X) \cdots p_k(X)$.*

DEMOSTRACIÓN: Basta aplicar sucesivamente el teorema anterior. De hecho, usando 1.33 es fácil probar que la descomposición es única salvo el orden. ■

Derivadas Terminamos esta sección introduciendo el concepto de derivada formal de un polinomio:

Definición 1.36 La derivada de un polinomio

$$p^n(X) = p_0 + p_1X + \cdots + p_{n-1}X^{n-1} + p_nX^n$$

es el polinomio

$$p'(X) = p_1 + 2p_2X + \cdots + (n-1)p_{n-1}X^{n-2} + np_nX^{n-1}.$$

Aquí hay que entender que la derivada de un polinomio constante p_0 es 0.

Una derivada puede volverse a derivar. Usaremos la notación $p^{k)}(X)$ para referirnos al polinomio que resulta de derivar k veces $p(X)$. Convendremos en que $p^{0)}(X) = p(X)$.

Una comprobación rutinaria nos da las propiedades siguientes:

[18] Observemos que la formalización de este teorema consiste en un esquema teoremático para cada $p^n(X)$ que es la disyunción de tantas fórmulas como descomposiciones posibles $n = n_1 + \cdots + n_k$, cada una de las cuales afirma la existencia de $\bar{p}^1_{n_1} \cdots \bar{p}^k_{n_k}$ tales que $p^n(X)$ es el producto de los polinomios irreducibles $p^{i,n_i}(X)$.

1. $(p(X) + q(X))' = p'(X) + q'(X)$,
2. $(c\, p(X))' = c\, p'(X)$,
3. $(p(X)q(X))' = p'(X)q(X) + p(X)q'(X)$.

Una inducción a partir de la fórmula del producto nos da la fórmula de Leibniz para derivadas sucesivas:

$$(p(X)q(X))^{k)} = \sum_{i=0}^{k} \binom{k}{i} p^{i)}(X)\; q^{k-i)}(X).$$

Una simple inducción sobre n prueba que la derivada del polinomio $(X-d)^m$ es $m(X-d)^{m-1}$, luego la derivada i-ésima es

$$m(m-1)\cdots(m-i+1)(X-d)^{m-i}.$$

Por lo tanto, la derivada k-ésima de $p(X) = p_n(X-d)^m\; q(X)$ es

$$p^{k)}(X) = p_n \sum_{i=0}^{k} \binom{k}{i} m(m-1)\cdots(m-i+1)(X-d)^{m-i}\; q^{k-i)}(X).$$

Vemos entonces que si $k < m$ se cumple $p^{k)}(d) = 0$, mientras que para $k = m$ tenemos

$$p^{m)}(d) = p_n\, m!\; q(d).$$

Si no suponemos el axioma **Car0** podría ocurrir que $m! = 0$. Con este axioma concluimos:

Teorema 1.37 ($\mathbf{C_0}$) *En las condiciones del teorema* 1.27, *el número m es el menor natural tal que $p^{m)}(d) \neq 0$. Además $p^{m)}(d) = p_n\, m!\; q(d)$.*

1.5 Extensiones algebraicas

Fijemos un número natural $n \geq 2$ y vamos a trabajar bajo la hipótesis de que el polinomio $d(X) \equiv d_1^n(X)$ es irreducible.

Consideramos de nuevo el espacio vectorial k^n estudiado en la sección 1.3, pero ahora, en lugar de representar los vectores mediante $\bar{v} = (v_1, \ldots, v_n)$, usaremos letras griegas y empezaremos a contar los índices en 0, es decir, que usaremos la notación $\alpha = (a_0, \ldots, a_{n-1})$. Esto es un mero cambio de notación que no afecta a la teoría.

Recordemos que si $\alpha = (a_0, \ldots, a_{n-1})$ y $\beta = (b_0, \ldots, b_{n-1})$, tenemos definida la suma

$$\alpha + \beta \equiv (a_0 + b_0, \ldots, a_{n-1} + b_{n-1}).$$

y el producto por un escalar

$$a\alpha = (aa_0, \ldots, aa_{n-1}),$$

de forma que se cumplen los axiomas de espacio vectorial. Ahora vamos a definir un producto $\alpha\beta$, para lo cual consideramos la división euclídea (véase la nota tras el teorema 1.24):

$$p^{2n-2}(X) = d_1^n(X)c_{2n+2,n}(X) + r_{2n-2,n}(X),$$

donde $\bar{r}_{2n-2,n}(\bar{p}_{2n-2}, \bar{d}_{n-1})$ es un multitérmino completamente determinado por el número natural n. Definimos[19]

$$\alpha\beta = \bar{r}_{2n-2,n}(\sum_{i+j=0} a_i b_j, \ldots, \sum_{i+j=2n-2} a_i b_j, \bar{d}).$$

Notemos que los términos que hemos introducido en lugar de las variables $\bar{p}_{2n-2}$ son los coeficientes del producto

$$\alpha^{n-1}(X)\beta^{n-1}(X) = \sum_{k=0}^{2n-2} \Big(\sum_{i+j=k} a_i b_j \Big) X^k,$$

luego $\alpha\beta$ son los coeficientes del resto de la división de este polinomio entre $d_1^n(X)$. Más explícitamente,

$$\alpha^{n-1}(X)\beta^{n-1}(X) = d(X)\bar{c}(X) + (\alpha\beta)^{n-1}(X),$$

y, por el teorema 1.24, $\alpha\beta$ es la única sucesión de longitud $n-1$ (empezando en 0) que cumple esta fórmula.

Ejemplo Consideremos el caso $n = 2$ y supongamos, pues, que el polinomio $X^2 + bX + c$ es irreducible. La división euclídea es

$$d_0 + d_1X + d_2X^2 = (c + bX + X^2)d_2 + d_0 - cd_2 + (d_1 - bd_2)X,$$

luego $r_0 = d_0 - cd_2$, $r_1 = d_1 - bd_2$ y en estos términos tenemos que sustituir $d_0 = a_0b_0$, $d_1 = a_0b_1 + a_1b_0$, $d_2 = a_1b_1$. El resultado es:

$$(a_0, a_1)(b_0, b_1) = (a_0b_0 - ca_1b_1, a_0b_1 + a_1b_0 - ba_1b_1).$$

■

Definimos $a^* \equiv (a, 0, \ldots, 0)$, de modo que ahora el vector $\bar{0}$ se expresa alternativamente como 0^*.

Teorema 1.38 *Si el polinomio $d_1^n(X)$ es irreducible, se cumple:*

1. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$,
2. $\alpha + \beta = \beta + \alpha$,
3. $\alpha + 0^* = \alpha$,
4. $\alpha + (-\alpha) = 0^*$,

[19]Observemos que si α y β son multivariables, entonces $\alpha\beta$ así definido es un multitérmino formado exclusivamente por sumas y productos de variables (y el relator $-$).

5. $(\alpha\beta)\gamma = \alpha(\beta\gamma)$,

6. $\alpha\beta = \beta\gamma$,

7. $\alpha \cdot 1^* = \alpha$,

8. $\alpha \neq 0^* \to \bigvee\beta\ \alpha\beta = 1^*$,

9. $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$,

10. $0^* \neq 1^*$.

Demostración: Las propiedades de la suma son las que ya hemos probado al estudiar los vectores. La propiedad 10. es trivial.

5. Por definición,

$$\alpha(X)\beta(X) = d(X)c(X)+(\alpha\beta)(X), \quad (\alpha\beta)(X)\gamma(X) = d(X)c'(X)+((\alpha\beta)\gamma)(X).$$

Por consiguiente,

$$\alpha(X)\beta(X)\gamma(X) = d(X)\ (c(X)\gamma(X) + c'(X)) + ((\alpha\beta)\gamma)(X).$$

En definitiva, tenemos que

$$\alpha(X)\beta(X)\gamma(X) = d(X)\ c''(X) + ((\alpha\beta)\gamma)(X),$$

para cierto polinomio $c''(X)$, e igualmente obtenemos que

$$\alpha(X)\beta(X)\gamma(X) = d(X)\ c'''(X) + (\alpha(\beta\gamma))(X),$$

para otro polinomio $c'''(X)$. El teorema 1.24 implica que $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

Las propiedades 6., 7. y 9. se prueban análogamente. Veamos, no obstante, la propiedad 7:

$$\alpha(X)1^*(X) = \alpha(X) = d(X) \cdot 0 + \alpha(X),$$

luego $\alpha \cdot 1^* = \alpha$.

La propiedad 8. es la única que requiere la hipótesis de que $d(X)$ es irreducible. En primer lugar, como $\alpha \neq 0$, podemos usar el teorema 1.23 para expresar $\alpha(X) = a_k\, p_1^k(X)$, con $k < n$ y $a_k \neq 0$. A continuación aplicamos 1.32, que nos asegura que, o bien $d(X) \mid p_1^k(X)$, o bien tenemos una ecuación

$$u(X)d(X) + v(X)p_1^k(X) = 1.$$

Descartamos el primer caso, pues significa que $p_1^k(X) = d(X)c'(X)$, luego

$$\alpha(X) = d(X)a_k c'(X) + 0^*(X),$$

y por otra parte

$$\alpha(X) = d(X) \cdot 0 + \alpha(X),$$

luego por la unicidad del resto tiene que ser $\alpha = 0^*$. Así pues:

$$a_k^{-1} v(X)\alpha(X) = -u(X)d(X) + 1.$$

Sea $\beta(X)$ el resto de la división

$$a_k^{-1} v(X) = d(X)c(x) + \beta^{n-1}(X).$$

Sustituimos en la ecuación precedente:

$$(d(X)c(X) + \beta(X))\alpha(X) = -u(X)d(X) + 1,$$

lo cual equivale a

$$\alpha(X)\beta(X) = d(X)(-u(X) - c(X)\alpha(X)) + 1,$$

luego $\alpha\beta = 1$. ■

Definición 1.39 Un *cuerpo* es una clase en la que hay definida una suma y un producto que cumplen los axiomas de C.

En estos términos, hemos probado que cada polinomio mónico irreducible de grado n define en el espacio vectorial k^n un producto con el que se convierte en un cuerpo. Es claro entonces que podemos aplicar a los elementos de k^n todos los teoremas de C.

Es fácil ver que se cumplen las propiedades siguientes:

1. $a^* = b^* \leftrightarrow a = b$,
2. $(a + b)^* = a^* + b^*$,
3. $(ab)^* = a^* b^*$.

Esto significa esencialmente que la aplicación $* : k \longrightarrow k^n$ dada por $a \mapsto a^*$ nos permite identificar a los números de k con parte de los elementos de k^n. A partir de ahora, llamaremos *"números del cuerpo base"* a los que hasta ahora llamábamos simplemente "números", es decir, a los elementos de k, mientras que los objetos representados por las multivariables $\alpha, \beta, \ldots$ podemos llamarlos los *números algebraicos* asociados al polinomio irreducible $d(X)$.

Veamos ahora que $a^*(a_0, \ldots, a_{n-1}) = (aa_0, \ldots, aa_{n-1})$.

En efecto, si llamamos $\alpha = (a_0, \ldots, a_{n-1})$, tenemos que

$$a^*(X)\alpha(X) = a \sum_{i=0}^{n-1} a_i X^i = \sum_{i=0}^{n-1} aa_i X^i,$$

y como es un polinomio de grado $n - 1$, se cumple que $a^*\alpha = (aa_0, \ldots, aa_{n-1})$.

Esto significa que, si identificamos cada número a del cuerpo base con el número $(a, 0, \ldots, 0)$ de la extensión algebraica, el producto de la estructura de cuerpo de k^n se restringe al producto por un escalar de la estructura vectorial de k^n.

Definimos $\xi \equiv (0, 1, 0, \ldots, 0)$, de modo que $\xi(X) = X$, de donde se sigue inmediatamente que $\xi^i = (0, \ldots 1, \ldots 0)$ (con el 1 en la posición i-ésima). Los dos últimos resultados implican que

$$(a_0, \ldots, a_{n-1}) = \sum_{i=0}^{n-1} a_i^* \xi^i.$$

Si admitimos el abuso de notación de suprimir los asteriscos, lo que tenemos es que cada número del cuerpo k^n se expresa de forma única como polinomio en ξ de grado menor que n con coeficientes en el cuerpo base.

Por ello, en lo sucesivo, cuando consideremos a k^n con estructura de cuerpo, lo representaremos con la notación $k[\xi]$. En particular, $\dim k[\xi] = n$.

Más concretamente, hemos probado que las potencias $1, \xi, \ldots, \xi^{n-1}$ no son sino la base canónica de $k[\xi]$ como espacio vectorial sobre k.

Como ya hemos señalado, podemos aplicar a $k[\xi]$ toda la teoría desarrollada en C. En particular podemos considerar polinomios con coeficientes en la extensión algebraica. Para distinguirlos, representaremos por $k[X]$ el conjunto de los polinomios con coeficientes en k y por $k[\xi][X]$ a los polinomios con coeficientes en $k[\xi]$. Esto significa tan sólo que, cuando hablemos de "un polinomio de $k[X]$" nos referiremos a $p^m(X)$, es decir, a una sucesión de números $(p_0, \ldots, p_m)$, mientras que si hablamos de "un polinomio de $k[\xi][X]$, nos referimos a una sucesión $(\alpha_0, \ldots, \alpha_m)$, donde cada α_i es a su vez una sucesión de n números.

Para cada polinomio $\bar{p}^m(X) \in k[X]$, podemos considerar el polinomio

$$p^{m*}(X) = p_0^* + p_1^* X + \cdots + p_m^* X^m \in k[\xi][X],$$

que, suprimiendo los asteriscos, representaremos simplemente por $p^m(X)$, pero ahora tiene sentido evaluarlo en números de $k[\xi]$. En estos términos, antes hemos probado que

$$\alpha = \alpha(\xi),$$

es decir, que si partimos de $\alpha = (a_0, \ldots, a_{n-1})$, consideramos el polinomio $\alpha(X) = a_0 + a_1 X + \cdots a_{n-1} X^{n-1}$, lo identificamos con $a_0^* + a_1^* X + \cdots a_{n-1}^* X^{n-1}$ y lo evaluamos en ξ, obtenemos $a_0 + a_1 \xi + \cdots + a_{n-1} \xi^{n-1} = \alpha$.

Seguidamente observamos que

$$\xi^{n-1}(X)\xi(X) = X^n = d(X) \cdot 1 - d_0 - d_1 X - \cdots - d_{n-1} X^{n-1},$$

luego $\xi^n = (-c_0, \ldots, -c_{n-1}) = -c_0 - c_1 \xi - \cdots - c_{n-1} \xi^{n-1}$, luego

$$d(\xi) = c_0 + c_1 \xi + \cdots + c_{n-1} \xi^{n-1} + \xi^n = 0.$$

El polinomio $d(X)$ no tiene raíces en el cuerpo base, porque es irreducible y tiene grado ≥ 2, y ahora vemos que lo que hemos construido es una extensión $k[\xi]$ en la que tiene una raíz ξ. Por ello nos referiremos a $k[\xi]$ como "la *adjunción* a k de una raíz del polinomio (mónico e irreducible) $d(X)$".

Este proceso de construcción de una extensión algebraica puede repetirse tomando a $k[\xi]$ como cuerpo base. Concretamente, si un polinomio $e^m(X)$ es irreducible en $k[\xi][X]$, podemos construir un cuerpo $k[\xi, \xi']$ en el que tiene una raíz ξ'.

Concretamente, cada $\omega \in k[\xi, \xi']$ es una sucesión $\omega = (\alpha_0, \ldots, \alpha_{m-1})$, donde a su vez $\alpha_i = (a_{i0}, \ldots, a_{i,n-1})$. Alternativamente, lo podemos representar de la forma

$$\omega = \sum_{j=0}^{m-1} \alpha_j \xi'^j,$$

donde a su vez $\alpha_j = \sum\limits_{i=0}^{n} a_{ij}\xi^i$, por lo que

$$\omega = \sum_{j=0}^{m-1} \sum_{i=0}^{n-1} a_{ij}\xi^i \xi'^j.$$

Sabemos que $k[\xi, \xi']$ cumple los axiomas de espacio vectorial con escalares en $k[\xi]$, pero es inmediato comprobar que también los cumple con escalares sobre k. La expresión que acabamos de obtener muestra que

$$k[\xi, \xi'] = \left\langle \xi^i \xi'^j \mid i = 0, \ldots, n-1, j = 0, \ldots, m-1 \right\rangle.$$

Veamos ahora que las potencias $\xi^i \xi'^j$ son linealmente independientes sobre k. Para ello suponemos que

$$\sum_{j=0}^{m-1} \sum_{i=0}^{n-1} a_{ij}\xi^i \xi'^j = 0,$$

con lo que la independencia lineal de los ξ'^j sobre $k[\xi]$ implica que

$$\sum_{i=0}^{n-1} a_{ij}\xi^i \xi'^j = 0, \qquad j = 0, \ldots, m-1,$$

y la independencia de los ξ^i sobre k implica que $a_{ij} = 0$.

Por lo tanto, las potencias $\xi^i \xi'^j$ son una base de $k[\xi, \xi']$, y en particular $\dim_k k[\xi, \xi'] = nm$.

Observemos que los elementos de $k[\xi, \xi']$ no son formalmente más complejos o más abstractos que los de $k[\xi]$, sino que, en lugar de ser vectores de n componentes, son vectores de nm componentes, con un producto que puede definirse explícitamente a partir de las nm coordenadas de cada factor.

El proceso puede repetirse cuantas veces se quiera para formar extensiones algebraicas de la forma $K = k[\xi_1, \ldots, \xi_n]$, donde cada ξ_i es raíz de un polinomio mónico irreducible de $k[\xi_1, \ldots, \xi_{i-1}][X]$. Se cumple entonces que K es un espacio vectorial cuya dimensión sobre k es el producto de las dimensiones de cada extensión sobre su precedente. Dicha dimensión recibe el nombre de *grado* de la extensión K (sobre k) y lo representaremos por $|K : k|$.

Es claro entonces que si tenemos una cadena de extensiones $k \subset K \subset L$ (cada una de las cuales se obtiene de adjuntar sucesivamente a la anterior un número finito de raíces de polinomios irreducibles), se cumple la relación de *transitividad de grados:*

$$|L:k| = |L:K||K:k|.$$

Teorema 1.40 *Si $p^m(X)$ es un polinomio irreducible en $k[X]$ y tiene una raíz ζ en una extensión algebraica K de k, entonces ζ no es raíz de ningún polinomio $q(X) \in k[X]$ no nulo de grado $k < m$.*

DEMOSTRACIÓN: Sea $u > 0$ el menor natural[20] tal que ζ es raíz de un polinomio de grado u, digamos $q_1^u(X)$. Dividimos $p(X) = q(X)c(X) + r(X)$, con $\operatorname{grad} r(X) < u$ y, como $r(\zeta) = 0$, tiene que ser $r(X) = 0$. Por lo tanto $q(X) \mid p(X)$, pero como $p(X)$ es irreducible y $q(X)$ no puede ser constante (o no tendría raíces), $q(X)$ tiene que ser asociado a $p(X)$, luego $u = m$. ■

Teorema 1.41 *Si K es una extensión algebraica de grado n y $\zeta \in K$, existe un único polinomio mónico irreducible $p(X) \in k[X]$ tal que $p(\zeta) = 0$. Además su grado es $\leq n$ y divide a cualquier otro polinomio de $k[X]$ que tenga a ζ por raíz.*

DEMOSTRACIÓN: Como K es un espacio vectorial de dimensión n sobre k, las potencias $1, \zeta, \ldots, \zeta^n$ no pueden ser linealmente independientes. Esto significa que existen escalares $a_0, \ldots, a_n \in k$ no todos nulos tales que

$$a_0 + a_1\zeta + \cdots + a_n\zeta^n = 0.$$

Equivalentemente, existe un polinomio $q^n(X) \in k[X]$ no nulo tal que $q^n(\zeta) = 0$. Por el teorema 1.35 sabemos que $q^n(X)$ se descompone en producto de polinomios irreducibles, luego ζ tiene que ser raíz de uno de ellos, y no perdemos generalidad si lo suponemos mónico. Llamémoslo $p(X)$ (que ciertamente tendrá grado $\leq n$).

Si ζ es raíz de $u(X) \in k[X]$, dividimos $u(X) = p(X)c(X) + r(X)$ y, como el grado del resto es menor que el grado de $p(X)$, el teorema anterior nos da que $r(X) = 0$, luego $p(X) \mid u(X)$ y, si el polinomio $u(X)$ es mónico e irreducible, necesariamente $u(X) = p(X)$. ■

Definición 1.42 Si K es una extensión algebraica y $\zeta \in K$, llamaremos *polinomio mínimo* de $\zeta \in k[\xi]$ al único polinomio mónico irreducible $p(X) \in k[X]$ que tiene a ζ por raíz. Lo representaremos por $\operatorname{pol\,min}_k \zeta$.

Hemos visto que si $p(X) \in k[X]$ es cualquier polinomio que cumpla $p(\zeta) = 0$, entonces $\operatorname{pol\,min}_k \zeta \mid p(X)$. En particular, si $p(X)$ es mónico e irreducible, tiene que ser $p(X) = \operatorname{pol\,min}_k \zeta$.

[20]Esto se formaliza mediante la disyunción "ζ es raíz de un polinomio no nulo de grado u y de ninguno de grado menor" o "ζ es raíz de un polinomio no nulo de grado $u-1$ y de ninguno de grado menor" o ..., que desdobla la demostración en u casos.

Observemos que, como siempre, podemos sustituir el cuerpo base k por otro cualquiera, de modo que si tenemos una cadena de extensiones algebraicas $k \subset K \subset L$ y $\zeta \in L$, podemos considerar tanto $\operatorname{pol\,min}_k \zeta$ como $\operatorname{pol\,min}_K \zeta$. La relación entre ambos es que el segundo divide al primero, pues $\operatorname{pol\,min}_k \zeta \in K[X]$ tiene a ζ por raíz.

Si K es una extensión algebraica, $\zeta \in K$ y $d(X) = \operatorname{pol\,min}_k \zeta$ tiene grado $n \geq 2$ (si el grado fuera 1 significaría que $d(X) = X - \zeta \in k[X]$, con lo que $\zeta \in k$), podemos considerar, por una parte, la extensión algebraica $k[\xi]$ definida a partir de $d(X)$, cuyos elementos son sucesiones $\alpha = (a_0, \ldots, a_{n-1})$ de n números, que pueden representarse alternativamente como

$$\alpha = \alpha^{n-1}(\xi) = \sum_{i=0}^{n-1} a_i \xi^i.$$

Por otra parte, podemos considerar la variedad lineal

$$k[\zeta] = \langle 1, \zeta, \ldots, \zeta^{n-1} \rangle \leq K.$$

El hecho de que ζ no sea raíz de ningún polinomio de $k[X]$ de grado menor que n equivale claramente a que las potencias $1, \zeta, \ldots, \zeta^{n-1}$ son linealmente independientes sobre k, luego forman una base de $k[\zeta]$, de forma que sus elementos se expresan de forma única como

$$\omega = \sum_{i=0}^{n-1} a_i \zeta^i.$$

Por lo tanto, podemos definir una aplicación $F_{\xi,\zeta} : k[\xi] \longrightarrow k[\zeta]$ mediante

$$F_{\xi,\zeta}(a_0, \ldots, a_{n-1}) = \sum_{i=0}^{n-1} a_i \zeta^i$$

o, en otros términos,

$$F_{\xi,\zeta}\Big(\sum_{i=0}^{n-1} a_i \xi^i\Big) = \sum_{i=0}^{n-1} a_i \zeta^i.$$

Acabamos de justificar que es biyectiva, y además cumple

$$F_{\xi,\zeta}(\alpha + \beta) = F_{\xi,\zeta}(\alpha) + F_{\xi,\zeta}(\beta), \qquad F_{\xi,\zeta}(\alpha\beta) = F_{\xi,\zeta}(\alpha) F_{\xi,\zeta}(\beta).$$

En efecto, la igualdad para la suma se comprueba fácilmente, y la del producto también si recordamos que el producto en $k[\xi]$ está determinado por la relación

$$\alpha^{n-1}(X)\beta^{n-1}(X) = d(X)\bar{c}(X) + (\alpha\beta)^{n-1}(X).$$

Si en ella sustituimos X por ζ queda precisamente la propiedad del producto.

De aquí se sigue en particular que $k[\zeta]$ es un cuerpo.

Definición 1.43 Si K y L son dos cuerpos que contienen a un mismo cuerpo k como subcuerpo, un *k-isomorfismo* de cuerpos $F : K \longrightarrow L$ es una aplicación que, para todo α, $\beta \in K$, cumpla

$$F(\alpha+\beta) = F(\alpha) + F(\beta), \qquad F(\alpha\beta) = F(\alpha)F(\beta),$$

así como que $\bigwedge a \in k\ F(a) = a$.

En estos términos casi hemos demostrado el teorema siguiente:

Teorema 1.44 *Sean K y L dos extensiones algebraicas de un mismo cuerpo k, sea $d(X) \in k[X]$ un polinomio mónico irreducible y sean $\zeta_1 \in K$ y $\zeta_2 \in L$ dos raíces de $d(X)$. Entonces existe un k-isomorfismo de cuerpos $F : k[\zeta_1] \longrightarrow k[\zeta_2]$ que cumple $F(\zeta_1) = \zeta_2$.*

Demostración: Hemos probado que si $k[\xi]$ es la extensión de k construida a partir de $d(X)$, existen k-isomorfismos de cuerpos $F_{\xi,\zeta_1} : k[\xi] \longrightarrow k[\zeta_1] \subset K$ y $F_{\xi,\zeta_2} : k[\xi] \longrightarrow k[\zeta_2] \subset L$ que además cumplen $F_{\xi,\zeta_i}(\xi) = \zeta_i$. Es fácil ver entonces que $F = F_{\xi,\zeta_1}^{-1} \circ F_{\xi,\zeta_2} : k[\zeta_1] \longrightarrow k[\zeta_2]$ es un k-isomorfismo de cuerpos que cumple lo requerido. ■

Nota En las condiciones del teorema anterior, el k-isomorfismo F se extiende a una aplicación $\bar{F} : k[\zeta_1][X] \longrightarrow k[\zeta_2][X]$ que a cada polinomio $p(X) = \sum_{i=0}^{n} p_i X^i$ le asigna

$$\bar{F}(p)(X) = \sum_{i=0}^{n} F(p_i)X^i.$$

Si pensamos en $p(X)$ como una sucesión de coeficientes $\bar{p} = (p_0, \ldots, p_n)$, entonces $\bar{F}(\bar{p}) = (F(p_0), \ldots, F(p_n))$.

Como la suma y el producto de polinomios de $k[\zeta_i][X]$ se definen en términos de la suma y el producto de los cuerpos $k[\zeta_i]$ (con las mismas fórmulas para ambos cuerpos) y F conserva dicha suma y dicho producto, es inmediato comprobar que

$$\bar{F}(p+q)(X) = \bar{F}(p)(X) + \bar{F}(q)(X), \quad \bar{F}(pq)(X) = \bar{F}(p)(X)\bar{F}(q)(X).$$

■

Veamos ahora una aplicación importante de las derivadas:

Teorema 1.45 (C$_0$) *Si α es un número de una extensión algebraica K de k, entonces α es raíz simple de* $\operatorname{pol\,min}\alpha$, *es decir,* $\operatorname{pol\,min}\alpha = (x-\alpha)q(X)$, *donde $q(X) \in K[x]$ cumple $q(\alpha) \neq 0$.*

Demostración: Sea $p(X) = \operatorname{pol\,min}\alpha$. La clave está (y aquí usamos **Car0**), en que $p'(X)$ es un polinomio no nulo de menor grado, luego $p'(\alpha) \neq 0$, ya que en caso contrario tendría que ser múltiplo de $p(X)$, luego basta aplicar el teorema anterior. ■

Vamos a realizar ahora una construcción de la que extraeremos varias consecuencias. Antes conviene introducir un concepto:

Definición 1.46 Si K es una extensión algebraica, diremos que un polinomio $p(X)$ de grado n *se escinde* en $K[X]$ si existen $\zeta_1, \ldots, \zeta_n \in K$ tales que

$$p(X) = p_n(X - \zeta_1) \cdots (X - \zeta_n).$$

Razonando en C_0, partimos de un polinomio irreducible $d_1^n(X) \in k[X]$ de grado mayor que 1. A partir de él construimos la extensión algebraica $k[\xi_1]$, donde tiene una raíz ξ_1.

Ahora tomamos un polinomio irreducible $e^m(X) \in k[\xi_1][X]$ y construimos la extensión $k[\xi_1, \zeta_1]$, donde tiene una raíz ζ_1. Puede que no sea la única. Aplicando sucesivamente el teorema 1.26 en $k[\xi_1, \zeta_1]$ llegamos a que

$$e_1^m(X) = (X - \zeta_1) \cdots (X - \zeta_{r_1}) e_1'^{m'}(X),$$

donde $e_1'^{m'}(X) \in k[\xi_1, \zeta_1][X]$ es un polinomio sin raíces en $k[\xi_1, \zeta_1]$. Si no es constante, por 1.34 tiene un factor irreducible $f_1^k(X) \in k[\xi_1, \zeta_1][X]$, y podemos construir una extensión algebraica $k[\xi_1, \zeta_1, \zeta_{r_1+1}]$ de $k[\xi_1, \zeta_1]$ donde $f_1^k(X)$ tenga una raíz ζ_{r_1+1}. Aplicando el teorema 1.26 en $k[\xi_1, \zeta_{r_1+1}]$ llegamos a que

$$e_1^m(X) = (X - \zeta_1) \cdots (X - \zeta_{r_2}) e_1''^{m''}(X),$$

donde $e_1''^{m''}(X) \in k[\xi_1, \zeta_1, \zeta_{r_1+1}][X]$ es un polinomio sin raíces en $k[\xi_1, \zeta_1, \zeta_{r_1+1}]$ y $m'' < m'$.

Como el grado $m'' < m' < m$ va decreciendo, tras un número finito de pasos tenemos que llegar a una extensión $k[\xi_1, \zeta_1, \zeta_{r_1+1}, \ldots, \zeta_{r_l+1}]$ donde $e_1^m(X)$ se escinde:

$$e_1^m(X) = (X - \zeta_1) \cdots (X - \zeta_m).$$

El teorema 1.45 nos asegura que los ζ_i son distintos dos a dos. Ahora volvemos a $d_1^n(X)$ y le aplicamos el mismo proceso, con lo que llegamos a una extensión $K = k[\xi_1, \zeta_1, \ldots, \zeta_{r_{l+1}}, \xi_{s_1}, \ldots, \xi_{s_{t+1}}]$ donde

$$d_1^n(X) = (X - \xi_1) \cdots (X - \xi_n),$$

con los ξ_i distintos dos a dos.

Si $j \neq 1$, la ecuación $\xi_i + x\zeta_j = \xi_1 + x\zeta_1$ tiene una única solución en K, que podrá estar en k o no, luego la ecuación tiene a lo sumo una solución en k. Por lo tanto, las $(m-1)n$ ecuaciones tienen a lo sumo $(m-1)n$ soluciones en k. El axioma **Inf** (que es consecuencia de **Car0**) implica entonces que existe un $c \in k$ tal que

$$\xi_i + c\zeta_j \neq \xi_1 + c\zeta_1, \qquad i = 1, \ldots, n, \quad j = 2, \ldots, m.$$

Llamamos $\theta = \xi_1 + c\zeta_1 \in k[\xi_1, \zeta_1]$ y consideramos el cuerpo $k[\theta] \subset k[\xi_1, \xi_2]$.

Sea $d^*(X) = d^n(\theta - cX) = \sum_{i=0}^{n} d_i(\theta - cX)^i \in k[\theta][X]$. Observemos que $d^*(\zeta_1) = 0$ y $d^*(\zeta_j) \neq 0$ para $j = 2, \ldots, m$.

En efecto, $d^*(\zeta_1) = d^n(\theta - c\zeta_1) = d^n(\xi_1) = 0$, pero $d^*(\zeta_j) = d^n(\theta - c\zeta_j) \neq 0$, pues $\theta - c\zeta_j$ no es ninguna de las ξ_i, que son todas las raíces de $d^n(X)$.

Sea ahora $f(X) \in k[\theta][X]$ el máximo común divisor de $d^*(X)$ y $e_1^m(X)$, es decir, el polinomio mónico dado por el teorema 1.30. Sabemos que $f(X) \mid d^*(X)$, $f(X) \mid e_1^m(X)$ y $f(X) = u(X)d^*(X) + v(X)e_1^m(X)$, para ciertos polinomios $u(X), v(X) \in k[\theta][X]$.

Como $f(X) \mid e_1^m(X)$ (en principio en $k[\theta][X]$, luego también en $K[X]$), cada factor irreducible de $f(X)$ divide a $e_1^m(X)$, luego por el teorema 1.33 divide a uno de sus factores irreducibles, es decir, un $X - \zeta_j$. Ahora bien, entonces $f(\zeta_j) = 0$ y, como $f(X) \mid d^*(X)$, también $d^*(\zeta_j) = 0$, luego necesariamente $j = 1$. Esto significa que $f(X) = (X - \zeta_1)^k$, pero como $f(X) \mid e_1^m(X)$, es fácil ver que de hecho $f(X) = X - \zeta_1$. Como $f(X) \in k[\theta][X]$, concluimos que $\zeta_1 \in k[\theta]$ y, por definición de θ, también $\xi_1 \in k[\theta]$.

Como todo elemento de $k[\xi_1, \zeta_1]$ es combinación lineal de potencias $\xi_1^u \zeta_1^v$, concluimos que $k[\xi_1, \theta_1] = k[\theta]$.

Teniendo en cuenta que hemos tomado $k[\xi_1]$ como la adjunción a k de una raíz de un polinomio irreducible arbitrario y que $k[\xi_1, \zeta_1]$ lo hemos tomado como la adjunción a $k[\xi_1]$ de una raíz de un polinomio irreducible arbitrario, hemos probado el *teorema del elemento primitivo:*

Teorema 1.47 ($\mathbf{C_0}$) *Si $k[\xi]$ es la adjunción a k de una raíz de un polinomio irreducible $d_1^n(X) \in k[X]$ y $k[\xi, \zeta]$ es la adjunción a $k[\xi]$ de una raíz de un polinomio irreducible $e_1^m(X) \in k[\xi][X]$, existe un $\theta \in k[\xi, \zeta]$ tal que $k[\xi, \zeta] = k[\theta]$.*

Continuamos con la construcción general y aplicamos sucesivamente el teorema anterior a la sucesión de extensiones $K = k[\xi_1, \zeta_1, \ldots, \zeta_{r_{l+1}}, \xi_{s_1}, \ldots, \xi_{s_{t+1}}]$, para concluir que existe un $\theta \in K$ tal que $K = k[\theta]$. Sea $p(X) \in k[X]$ su polinomio mínimo y vamos a probar que $p(X)$ se escinde en $K[X]$.

En caso contrario $p(X)$ tendría un factor irreducible en $K[X]$ de grado mayor que 1, con el que podríamos formar una extensión algebraica $L = K[\theta']$, donde θ' sería una raíz de $p(X)$ fuera de K. El teorema 1.44 nos da un k-isomorfismo $F : K \longrightarrow k[\theta']$ tal que $F(\theta) = \theta'$.

Por otra parte, θ se puede expresar como combinación lineal con coeficientes en k de potencias $\xi_{r_i}^{u_i} \zeta_{s_j}^{v_j}$, luego $\theta' = F(\theta)$ es combinación lineal de potencias $F(\xi_{r_i})^{u_i} F(\zeta_{s_j})^{v_j}$.

Pero $d(\xi_{r_i}) = 0$, luego, al aplicar F a esta igualdad (teniendo en cuenta que F atraviesa las sumas y los productos y deja fijos a los coeficientes de d) resulta que $d(F(\xi_{r_i})) = 0$, luego $F(\xi_{r_i})$ es un ξ_j, luego $F(\xi_{r_i}) \in K$, e igualmente se razona que $F(\zeta_{s_j}) \in K$, luego $\theta' \in K$, contradicción.

Definición 1.48 Una extensión algebraica K es *normal* si es de la forma $k[\theta]$ y el polinomio mínimo de θ se escinde en $K[X]$.

En estos términos, teniendo en cuenta que $k[\xi_1]$ era una extensión algebraica arbitraria, hemos demostrado lo siguiente:

Teorema 1.49 *Toda extensión algebraica está contenida en una extensión algebraica normal.*

Teorema 1.50 *Si K es una extensión algebraica normal de un cuerpo k y $\zeta \in K$, entonces* $\operatorname{pol\,min}_k \zeta$ *se escinde en* $K[X]$.

Demostración: Sea $K = k[\theta]$ de modo que $p(X) = \operatorname{pol\,min}_k \theta$ se escinda en $K[X]$:

$$p(X) = (X - \theta_1) \cdots (X - \theta_n),$$

con $\theta_1 = \theta$.

Sea $q(X) = \operatorname{pol\,min}_k \zeta$ y supongamos que no se escinde en $K[X]$. Entonces tiene un factor irreducible de grado mayor que 1, a partir del cual podemos formar una extensión $L = K[\zeta']$ donde $q(X)$ tiene una raíz ζ' que no está en K. Por el teorema 1.44 existe un k-isomorfismo $F : k[\zeta] \longrightarrow k[\zeta']$.

Sea $p_0(X) = \operatorname{pol\,min}_{k[\zeta]}\theta \in k[\zeta][X]$, que es un factor mónico irreducible de $p(X)$ en $k[\zeta][X]$ y $p_0(\theta) = 0$.

Según la nota tras 1.44, si llamamos $p_0^*(X) = \bar{F}(p_0(X)) \in k[\zeta'][X]$, como $p_0(X) \mid p(X)$, también $p_0^*(X) \mid \bar{F}(p(X)) = p(X)$ ($\bar{F}$ no afecta a $p(X)$ porque éste tiene sus coeficientes en k), luego un factor irreducible de $p_0^*(X)$ en $L[X]$ debe coincidir con uno de los factores irreducibles de $p(X)$, que son los $X - \theta_i$. En definitiva, existe un $\theta' = \theta_i$ tal que $p_0^*(\theta') = 0$.

Como $K = k[\theta]$, se comprueba inmediatamente que $K = k[\zeta][\theta]$ y, si el polinomio $p_0(X) = \operatorname{pol\,min}_{k[\zeta]} \theta$ tiene grado d, cada $\omega \in K = k[\theta]$ se expresa de forma única como

$$\omega = \sum_{i=0}^{d-1} \alpha_i \theta^i,$$

con $\alpha_i \in k[\zeta]$ o, equivalentemente, $\omega = p^{d-1}(X)$, para cierto $p^{d-1}(X) \in k[\zeta][X]$. Por lo tanto, podemos definir $F^* : K \longrightarrow L$ mediante

$$F^*\Big(\sum_{i=0}^{d-1} \alpha_i \theta^i\Big) = \sum_{i=0}^{d-1} F(\alpha_i)\theta'^i,$$

que claramente extiende a $F : k[\zeta] \longrightarrow k[\zeta']$. En particular, sigue cumpliéndose que $F^*(\zeta) = \zeta'$ y además $F^*(\theta) = \theta'$.

Observemos que una expresión alternativa para F^* en términos de la extensión $\bar{F} : k[\zeta][X] \longrightarrow k[\zeta'][X]$ definida tras el teorema 1.44 es

$$F^*(p^{d-1}(\theta)) = \bar{F}(p^{d-1})(\theta').$$

Teniendo esto en cuenta es fácil ver que F^* es un k-isomorfismo de cuerpos. La conservación de las sumas es inmediata y, para el producto, tomamos dos números $\omega = f^{d-1}(\theta)$ y $\omega' = g^{d-1}(\theta)$, con $f^{d-1}(X), g^{d-1}(X) \in k[\zeta][X]$, dividimos

$$f^{d-1}(X)g^{d-1}(X) = p_0(X)c(X) + r^{d-1}(X),$$

de modo que $\omega\omega' = r^{d-1}(\theta)$. Aplicamos $\bar{F} : k[\zeta][X] \longrightarrow k[\zeta'][X]$, con lo que

$$\bar{F}(f^{d-1})(X)\bar{F}(g^{d-1})(X) = p_0^*(X)\bar{F}(c)(X) + \bar{F}(r^{d-1})(X),$$

y al evaluar en θ' resulta

$$F^*(\omega)F^*(\omega') = p_0^*(\theta')\bar{F}(c)(\theta') + F^*(\omega\omega') = F^*(\omega\omega').$$

Ahora bien, como $\zeta = h(\theta)$, para cierto polinomio $h(X) \in k[X]$, llegamos a que $\zeta' = F^*(\zeta) = h(F^*(\theta)) = h(\theta') \in K$, contradicción. ■

Definición 1.51 Si $K = k[\theta]$ es una extensión algebraica normal y $\theta_1, \ldots, \theta_n$ son las raíces de su polinomio mínimo, llamaremos *conjugaciones* de K a los k-isomorfismos $\sigma_j : K \longrightarrow K$ dados por

$$\alpha = \sum_{i=0}^{n} a_i\theta^i \mapsto \sigma_j(\alpha) = \sum_{i=0}^{n} a_i\theta_j^i,$$

Teorema 1.52 *Si $K = k[\theta]$ es una extensión algebraica normal de grado n, $\theta_1, \ldots, \theta_n$ son las raíces de su polinomio mínimo y $\zeta \in K$, entonces las raíces del polinomio mínimo de ζ son los conjugados $\sigma_i(\zeta)$.*

Demostración: Basta repetir el planteamiento de la prueba del teorema anterior, sólo que ahora $\zeta' \in K$ es otra raíz del polinomio mínimo de ζ. Como allí, podemos definir un isomorfismo de cuerpos sobre K que extiende al isomorfismo de $k[\zeta]$ en $k[\zeta']$, pero si dicho isomorfismo transforma θ en θ_j, entonces es necesariamente σ_j. ■

Capítulo II

La teoría elemental de cuerpos ordenados

En el capítulo precedente hemos visto una muestra de las matemáticas que pueden desarrollarse a partir únicamente de los axiomas de cuerpo. Sin embargo, el álgebra elemental no sólo incluye sumas y productos, sino también desigualdades. Ahora vamos a extender la teoría C para incorporar una relación de orden. En la primera sección estudiaremos de forma aislada los axiomas de orden y en la siguiente los combinaremos con los axiomas de cuerpo.

2.1 Conjuntos totalmente ordenados

Consideramos el lenguaje formal $\mathcal{L}_0$ cuyo único signo eventual es un relator diádico $\leq$. La *teoría de los conjuntos totalmente ordenados* es la teoría O sobre $\mathcal{L}_0$ cuyos axiomas son:

O1	$x \leq x$
O2	$x \leq y \land y \leq x \rightarrow x = y$
O3	$x \leq y \land y \leq z \rightarrow x \leq z$
O4	$x \leq y \lor y \leq x$

Escribiremos también $x \geq y$ en lugar de $y \geq x$. Definimos además

$$x < y \equiv y > x \equiv x \leq y \land x \neq y.$$

Por simplicidad nos restringiremos al caso que realmente nos va a interesar, que es el de la *teoría de los conjuntos ordenados densos no acotados,* que es la teoría DNA que resulta de añadir a O los axiomas:

D	$x < y \rightarrow \bigvee z(x < y < z)$
NA	$\bigvee yz\ y < x < z$

Es fácil ver que basta añadir **D** o **NA** a la teoría O para que se pueda probar el esquema de infinitud **Inf**.

Llamaremos *intervalos* a las clases siguientes:

$$]a,b[\, = \{x \mid a < x < b\}, \qquad [a,b] = \{x \mid a \leq x \leq b\},$$

$$[a,b[\, = \{x \mid a \leq x < b\}, \qquad]a,b] = \{x \mid a < x \leq b\},$$

$$]-\infty,b[\, = \{x \mid x < b\}, \quad]a,+\infty[\, = \{x \mid a < x\},$$

$$]-\infty,b] = \{x \mid x \leq b\}, \quad [a,+\infty[\, = \{x \mid a \leq x\}.$$

$$]-\infty,+\infty[\, = \{x \mid x = x\}.$$

Observemos que la clase vacía es un intervalo, pues $\varnothing = \,]a,a[$.

El teorema siguiente se demuestra sin dificultad distinguiendo casos:[1]

Teorema 2.1 *La intersección de dos intervalos es un intervalo.*

De aquí se sigue por inducción que la intersección de un número finito de intervalos es un intervalo y, por la propiedad distributiva de la unión y la intersección, que la intersección de dos uniones finitas de intervalos es una unión finita de intervalos.

Definición 2.2 Para cada clase A, definimos los conceptos siguientes:

- M es el *máximo* de A si $M \in A \land \bigwedge x \in A\; x \leq M$.
- m es el *mínimo* de A si $m \in A \land \bigwedge x \in A\; m \leq x$.
- c es *cota superior* de A si $\bigwedge x \in A\; x \leq c$.
- c es *cota inferior* de A si $\bigwedge x \in A\; c \leq x$.
- s es *supremo* de A si s es cota superior de A y

$$\bigwedge c(c \text{ es cota superior de } A \rightarrow s \leq c).$$

- i es *ínfimo* de A si i es cota inferior de A y

$$\bigwedge c(c \text{ es cota inferior de } A \rightarrow c \leq i).$$

- A está acotada superior/inferiormente si tiene una cota superior/inferior.

[1] En realidad el teorema es un esquema que engloba un número finito de teoremas distintos, como por ejemplo

$$]a,b[\,\cap\,[c,d[\, = \varnothing \;\lor\;]a,b[\,\cap\,[c,d[\, = \,]a,b[\;\lor\;]a,b[\,\cap\,[c,d[\, = [c,d[$$

$$\lor\;]a,b[\,\cap\,[c,d[\, = \,]a,d[\lor\;]a,b[\,\cap\,[c,d[\, = [c,b[\,.$$

Es fácil probar que si una clase tiene máximo, mínimo, supremo o ínfimo, éstos son únicos, así como que todo máximo es supremo y todo mínimo es ínfimo.

También es inmediato que todo intervalo con extremo superior/inferior infinito es no acotado superior/inferiormente, mientras que, si $a < b$, entonces b es el supremo de los intervalos $]a, b[$, $[a, b]$, $[a, b[$, $]a, b]$, $]-\infty, b]$, $]-\infty, b[$ y a es el ínfimo de los intervalos $]a, b[$, $[a, b]$, $[a, b[$, $[a, b[$, $]a, +\infty]$, $]a, +\infty[$.

El teorema siguiente se prueba fácilmente por inducción sobre n:

Teorema 2.3 $\bigvee m$ *m es el máximo de* $\{x_1, \ldots, x_n\}$.

Teorema 2.4 *Toda unión finita de intervalos no vacía que esté acotada superior/inferiormente tiene supremo/ínfimo.*

DEMOSTRACIÓN: Consideramos una unión finita $A = I_1 \cup \cdots \cup I_n$, donde cada I_i es un intervalo, que podemos suponer no vacío (pues de lo contrario se puede eliminar sin alterar la unión). Si está acotada superiormente, cada I_i tiene que tener extremo superior finito b_i, y podemos tomar el máximo s de todos los b_i, que existe por el teorema anterior. Veamos que s es el supremo de A. Para ello observamos que si $x \in A$, entonces existe un i tal que $x \in I_i$, luego $x \leq b_i \leq s$, y esto prueba que s es una cota superior de A.

Sea ahora c una cota superior de A, y veamos que $s \leq c$. Supongamos, por el contrario, que $c < s$. Sabemos que existe un i tal que $b_i = s$. Entonces $b_i \notin I_i$, pues de lo contrario tendría que ser $b_i = s \leq c$. Esto implica que I_i es de la forma $]a_i, b_i[$, $[a_i, b_i[$, $]-\infty, b_i[$, con $a_i < b_i$ en los dos primeros casos, o de lo contrario $I_i = \varnothing$.

Tomamos $u \in I_i$, de modo que $u \leq c < b_i = s$. Por **D** existe un x tal que $c < x < b_i$, y es claro entonces que $x \in I_i \subset A$, en contradicción con que c sea una cota superior de A.

El caso en que A está acotado inferiormente se razona de forma análoga. ■

2.2 Cuerpos ordenados

Definimos el *lenguaje formal del álgebra elemental* como el lenguaje $\mathcal{L}_A$ cuyos únicos signos eventuales son dos constantes $0, 1$, un funtor monádico $-$, dos funtores diádicos $+$ y $\cdot$ y un relator monádico "> 0" que leeremos como "es positivo", es decir, añadimos a $\mathcal{L}_A^-$ este último funtor.

La *teoría de los cuerpos ordenados* CO es la teoría axiomática sobre el lenguaje $\mathcal{L}_A$ cuyos axiomas son los de C más los axiomas siguientes:

CO1	$\neg(x > 0 \land -x > 0)$
CO2	$x = 0 \lor x > 0 \lor -x > 0$
CO3	$x > 0 \land y > 0 \to x + y > 0$
CO4	$x > 0 \land y > 0 \to xy > 0$

Definimos

$$x < y \equiv y > x \equiv y - x > 0, \qquad x \leq y \equiv y \geq x \equiv x < y \lor x = y.$$

Al trabajar en CO representaremos el cuerpo base con la letra R en lugar de k.

Teorema 2.5 *La relación $<$ es una relación de orden total estricto, es decir:*

1. $x < y \leftrightarrow x \leq y \land x \neq y$,
2. $x < y \lor y < x \lor x = y$, *y los tres casos son mutuamente excluyentes,*
3. $x < y \land y < z \to x < z$.

Demostración: 1. Obviamente $x \leq y \land x \neq y \to x < y$, por definición. Para probar la implicación contraria basta ver que $\neg x < x$. En efecto, esto equivale a que $\neg 0 > 0$, pero si fuera $0 > 0$, entonces también $-0 > 0$, en contra de **CO1**.

2. La disyunción se sigue inmediatamente de **CO2**. Los dos primeros casos no pueden darse a la vez por **CO1**, y el tercero no puede darse a la vez que uno de los dos primeros por 1.

3. Tenemos que $y - x > 0$, $z - y > 0$, luego **CO3** nos da que $z - x > 0$, es decir, $x < z$. ■

A partir de aquí se demuestra sin dificultad que $\leq$ es una relación de orden total no estricto, así como las versiones de **CO3** y **CO4** en términos de $\leq$:

Teorema 2.6 *Se cumple:*

1. $x \leq x$,
2. $x \leq y \land y \leq x \to x = y$,
3. $x \leq y \land y \leq z \to x \leq z$,
4. $x \leq y \lor y \leq x$,
5. $x \leq y \to x + z \leq y + z$,
6. $x \leq y \land z \geq 0 \to xz \leq yz$.

En particular, vemos que en CO se demuestran los axiomas de O. De aquí a su vez podemos deducir algunas propiedades adicionales:

Teorema 2.7 *Se cumple:*

1. $x \leq y \land z \leq w \to x + z \leq y + w$,
2. $x \leq y \to -y \leq -x$,
3. $x \leq y \land z < w \to x + z < y + w$,

4. $x^2 \geq 0$,

5. $-1 < 0 < 1$,

6. $x \leq y \land z \geq 0 \to xz \leq yz$,

7. $x \leq y \land z \leq 0 \to xz \geq yz$,

8. $0 < x < y \to 0 < 1/y < 1/x$,

9. $x + y = 0 \land x \geq 0 \land y \geq 0 \to x = y = 0$,

10. $x_1^2 + \cdots + x_n^2 = 0 \to x_1 = \cdots = x_n = 0$.

Demostración: 1. Por 5. del teorema anterior $x+z \leq y+z \land y+z \leq y+w$, y ahora se aplica 3).

2. Por 5. del teorema anterior $-y - x + x \leq -y - x + y$, luego $-y \leq -x$.

3. En caso contrario, por el teorema anterior sería $y + w \leq x + z$, por 2. (de este teorema) $-y \leq -x$, luego por 1. $w \leq z$, contradicción.

4. Por **CO2** tenemos que $x = 0 \lor x > 0 \lor -x > 0$, luego por **CO4** se cumple $x^2 = 0 \lor x^2 > 0 \lor (-x)^2 > 0$, luego $x^2 \geq 0$ en cualquier caso.

5. $1 = 1^2 \geq 0$ por 4., y la desigualdad estricta nos la da **C10**. De 2. se sigue entonces que $-1 < 0$.

6. Tenemos que $y - x \geq 0$, luego por 6. del teorema anterior $(y - x)z \geq 0$, de donde $xz \leq yz$.

7. Tenemos que $-z \geq 0$, luego por 6) $-xz \leq -yz$, luego por 2. $xz \geq yz$.

8. Si fuera $1/x < 0$, por 7. tendríamos que $1 = x(1/x) \leq 0$, contradicción. Por lo tanto, $1/x > 0$. Igualmente, $1/(xy) > 0$, luego por 6) $x/(xy) \leq y/(xy)$, es decir, $1/y \leq 1/x$. Si se diera la igualdad sería $x = y$, luego $1/y < 1/x$.

9. Como $0 \leq x$, también $0 \leq y \leq x + y = 0$, luego $y = 0$. Igualmente llegamos a que $x = 0$.

10. se demuestra por inducción sobre n a partir de la propiedad 9. (teniendo en cuenta que, por 4., los cuadrados son no negativos). ■

De las propiedades 3. y 5. deducimos que $x - 1 < x < x + 1$, y también es fácil ver que

$$x < y \to x < \frac{x+y}{2} < y,$$

luego en CO se demuestran todos los axiomas de la teoría DNA.

También a partir de las propiedades 3. y 5., una simple inducción demuestra que si dos números enteros cumplen $m < n$, entonces $\vdash_{\mathrm{CO}} m < n$.

En particular, en CO puede probarse como esquema teoremático el esquema axiomático **Car0**, luego CO extiende, de hecho, a C_0.

Definición 2.8 La teoría CP de los *cuerpos pitagóricos* es la que resulta de añadir a CO el axioma

$$\mathbf{P} \qquad \bigvee z\ x^2 + y^2 = z^2$$

que afirma que la suma de cuadrados es un cuadrado.

La teoría CE de los *cuerpos euclídeos* es la que resulta de añadir a CO el axioma

$$\mathbf{E} \qquad x \geq 0 \to \bigvee y\ x = y^2,$$

que afirma que todo número no negativo es un cuadrado.

Puesto que en CO se demuestra que todo cuadrado es no negativo, es claro que $\vdash_{\mathrm{CO}} \mathbf{E} \to \mathbf{P}$.

El valor absoluto En un cuerpo ordenado podemos definir como sigue[2] el valor absoluto de un número:

$$|x| = \begin{cases} x & \text{si } x \geq 0, \\ -x & \text{si } x < 0. \end{cases}$$

Teorema 2.9 *Se cumple:*

1. $|x| \leq y \leftrightarrow -y \leq x \leq y$,
2. $|x| \geq 0$,
3. $|x| = 0 \leftrightarrow x = 0$,
4. $|x + y| \leq |x| + |y|$,
5. $|xy| = |x|\,|y|$,
6. $y \neq 0 \to |x/y| = |x|/|y|$.

Demostración: 1. Supongamos que $|x| \leq y$ y distingamos dos casos: si $x \geq 0$, entonces $0 \leq x \leq y$, luego $-y \leq -x \leq 0 \leq x \leq y$. Si por el contrario $x < 0$, entonces $0 < -x \leq y$, luego $-y \leq x < 0 \leq y$.

Recíprocamente, si se cumple $-y \leq x \leq y$, entonces, multiplicando por -1, tenemos que $-y \leq -x \leq y$, y como $|x| = \pm x$, se cumple que $|x| \leq y$.

2. y 3. son inmediatos. Para probar 4. observamos que, como $|x| \leq |x|$, aplicando 1) resulta que $-|x| \leq x \leq |x|$, e igualmente $-|y| \leq y \leq |y|$. Por consiguiente $-|x| - |y| \leq x + y \leq |x| + |y|$, y de nuevo por 1. $|x + y| \leq |x| + |y|$.

5. y 6. se prueban sin dificultad. ■

[2] En principio, esto significa que $|x| = y \equiv (x \geq 0 \land y = x) \lor (x < 0 \land y = -x)$.

Números complejos En CO tenemos que el polinomio X^2+1 no tiene raíces, luego es irreducible y podemos formar la extensión algebraica $C = R[i]$ que resulta de adjuntar a R una raíz de dicho polinomio, cuyos elementos serán de la forma $z = a + bi$, con $i^2 = -1$. A los números de R los llamaremos *"números reales"* y los de C serán los *"números complejos"*.

El *conjugado* de un número complejo se define como $\overline{a + bi} = a - bi$. Una comprobación rutinaria muestra que

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2, \qquad \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2.$$

Alternativamente, podemos concluir que se cumplen estas propiedades porque C es una extensión algebraica normal (ya que $X^2 + 1 = (X + i)(X - i)$ se escinde en $C[X]$) y la conjugación que acabamos de definir es una de las dos conjugaciones definidas en general en 1.51.

Teorema 2.10 (CE) *Todo número complejo es un cuadrado.*

Demostración: Observemos en primer lugar que todo $x \in R$ tiene raíz cuadrada en C, pues si $x \geq 0$ la tiene en R y si $x < 0$, entonces $-x > 0$, luego existe un $y \in R$ tal que $-x = y^2$, y entonces $(yi)^2 = x$.

Tomamos ahora un número complejo $z = a + bi$. Como $a^2 + b^2 \geq 0$, existe $c \in R$ tal que $c^2 = a^2 + b^2$. Sean $u, v \in C$ tales que

$$u^2 = \frac{c + a}{2}, \qquad v^2 = \frac{c - a}{2}.$$

Entonces $u^2 - v^2 = a$ y $4u^2v^2 = b^2$, luego $2uv = \pm b$. Cambiando si es preciso u por $-u$ se sigue cumpliendo la primera ecuación, y la segunda se convierte en $2uv = b$. Por lo tanto:

$$(u + vi)^2 = u^2 - v^2 + 2uvi = a + bi.$$

■

Teorema 2.11 (CE) *Se cumple:*

1. *El polinomio $aX^2 + bX + c \in R[X]$ con $a \neq 0$ tiene una raíz en R si y sólo si $b^2 - 4ac \geq 0$.*
2. *Todo polinomio en $C[X]$ de grado 2 tiene una raíz en C.*

Demostración: Que un número x sea raíz del polinomio equivale a que

$$4a^2x^2 + 4abx + 4ac = 0 \quad \Leftrightarrow \quad (2ax + b)^2 = b^2 - 4ac,$$

luego $p(X)$ tiene una raíz en R si y sólo si $\bigvee d\, d^2 = b^2 - 4ac$. En CE esto equivale a que $b^2 - 4ac \geq 0$.

Por otra parte, este mismo argumento (partiendo ahora de un polinomio en $C[X]$) junto con el teorema anterior implica que siempre existe una raíz en C.

■

Continuidad El teorema siguiente afirma que los polinomios son funciones continuas, y a continuación extraemos varias consecuencias de este hecho:

Teorema 2.12

$$\bigwedge\epsilon > 0\bigvee\delta > 0\bigwedge x(|x - x_0| < \delta \rightarrow |p^n(x) - p^n(x_0)| < \epsilon).$$

DEMOSTRACIÓN: Llamaremos $C(p_0, \ldots, p_n; x_0)$ al enunciado del teorema. Observemos que $C(p_0; x_0)$ se cumple trivialmente. Vamos a demostrar que se cumple $C(0, \ldots, 0, p_n; x_0)$ por inducción sobre n, es decir, se trata de probar que

$$\bigwedge\epsilon > 0\bigvee\delta > 0\bigwedge x(|x - x_0| < \delta \rightarrow |p_n x^n - p_n x_0^n| < \epsilon).$$

Lo tenemos probado para $n = 0$. Supongamos que es cierto para n y tomemos $\epsilon > 0$. Entonces

$$|o_n x^{n+1} - p_n x_0^{n+1}| = |p_n x^{n+1} - p_n x^n x_0 + p_n x^n x_0 - p_n x_0^{n+1}|$$
$$\leq |p_n x^n||x - x_0| + |x_0||p_n x^n - p_n x_0^n|.$$

Por hipótesis de inducción existe un $\delta > 0$ tal que si $|x - x_0| < \delta$, entonces

$$|p_n x^n - p_n x_0^n| < \frac{\epsilon}{2(|x_0| + 1)}.$$

En particular

$$|p_n x^n| = |p_n x^n - p_n x_0^n + p_n x_0^n| \leq |p_n x^n - p_n x_0^n| + |p_n x_0^n| < \frac{\epsilon}{2(|x_0| + 1)} + |p_n x_0^n|.$$

Como δ puede sustituirse por cualquier otro número positivo menor, podemos suponer que

$$0 < \delta < \frac{\epsilon}{2(\frac{\epsilon}{2(|x_0|+1)} + |p_n x_0^n| + 1)}.$$

Así, si $|x - x_0| < \delta$, se cumple que

$$|p_n x^{n+1} - p_n x_0^{n+1}| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Ahora probamos el teorema por inducción sobre n. Lo tenemos probado para $n = 0$. Si vale para n, fijamos $\epsilon > 0$ y observamos que

$$|p_0 + p_1 x + \cdots + p_{n+1} x^{n+1} - (p_0 + p_1 x_0 + \cdots + p_{n+1} x_0^{n+1})| \leq$$
$$|p_0 + p_1 x + \cdots + p_n x^n - (p_0 + p_1 x_0 + \cdots + p_n x_0^n)| + |p_{n+1} x^{n+1} - p_{n_1} x_0^{n+1}|.$$

Por hipótesis de inducción existe un $\delta_1 > 0$ tal que si $|x - x_0| < \delta_1$, entonces el primer sumando es menor que $\epsilon/2$, y por lo que acabamos de probar existe otro $\delta_2 > 0$ tal que si $|x - x_0| < \delta_2$, entonces el segundo sumando es menor que $\epsilon/2$. Claramente entonces, basta tomar como δ el mínimo de ambos. ■

En realidad lo que necesitaremos será la consecuencia siguiente de la continuidad:

Teorema 2.13 $p^n(x_0) > 0 \rightarrow \bigvee ab(a < x_0 < b \wedge \bigwedge x(a < x < b \rightarrow p^n(x) > 0))$.

DEMOSTRACIÓN: Basta tomar $\epsilon = p_0 + p_1x_0 + \cdots + p_nx_0^n$ y aplicar el teorema anterior, que nos da un $\delta > 0$ tal que si $|x - x_0| < \delta$ entonces

$$|p_0 + p_1x + \cdots + p_nx^n - \epsilon| < \epsilon,$$

lo cual implica implica que

$$-\epsilon < p_0 + p_1x + \cdots + p_nx^n - \epsilon < \epsilon.$$

Entonces $a = x_0 - \delta$ y $b = x_0 + \delta$ cumplen lo requerido. ■

Este teorema es un caso particular del teorema siguiente:

Teorema 2.14 *Si $p(X)$ es un polinomio no nulo de grado n, existe un mínimo natural $m \leq n$ tal que $p^{m)}(d) \neq 0$, y entonces:*

1. *Si m es impar y $p^{m)}(d) > 0$,*
$$\bigvee\delta > 0 \bigwedge xy(d - \delta < x < d < y < d + \delta \rightarrow p(x) < 0 < p(y)).$$
2. *Si m es impar y $p^{m)}(d) < 0$,*
$$\bigvee\delta > 0 \bigwedge xy(d - \delta < x < d < y < d + \delta \rightarrow p(y) < 0 < p(x)).$$
3. *Si m es par y $p^{m)}(d) > 0$,*
$$\bigvee\delta > 0 \bigwedge x(|x - d| < \delta \rightarrow p(x) > 0).$$
4. *Si m es par y $p^{m)}(d) < 0$,*
$$\bigvee\delta > 0 \bigwedge x(|x - d| < \delta \rightarrow p(x) < 0).$$

DEMOSTRACIÓN: La existencia de m la proporcionan los teoremas 1.27 y 1.37, que nos dan además[3] que $p(X) = (X - d)^m q(X)$, para cierto polinomio $q(X)$ tal que $q(d) \neq 0$, y $p^{m)}(d) = m!\, q(d)$.

Por el teorema anterior existe un $\delta > 0$ tal que si $|x - d| < \delta$ entonces el signo de $q(X)$ coincide con el de $p^{m)}(d)$, y la conclusión en cada caso sólo requiere discutir el signo de $(x - d)^m$, que para $x < d$ depende obviamente de la paridad de m. ■

Teorema 2.15 *Si n es un número natural, se cumple:*

$$\bigvee M > 0(\bigwedge x(x > M \rightarrow p_1^n(x) > 0) \wedge \bigwedge x(x < -M \rightarrow (-1)^n p_1^n(x) > 0)).$$

[3]Por comodidad hemos incorporado el coeficiente p_n al polinomio $q(X)$, que en los teoremas citados se suponía mónico.

Demostración: Si $x \neq 0$, podemos expresar

$$p_n(x) = p_0 + p_1 x + \cdots + p_{n-1}x^{n-1} + x^n = x^n \left(\frac{p_0}{x^n} + \frac{p_1}{x^{n-1}} + \cdots + \frac{p_{n-1}}{x} + 1 \right).$$

Tomemos M tal que $M > 1$ y $M > n|p_i|$, para todo i. Entonces, si $|x| \geq M$, tenemos que $|x|^{n-i-1} \geq 1$, luego $|x|^{n-i} > n|p_i|$, luego

$$\frac{|p_i|}{|x|^{n-i}} < \frac{1}{n},$$

luego

$$\left| \frac{p_0}{x^n} + \frac{p_1}{x^{n-1}} + \cdots + \frac{p_{n-1}}{x} \right| \leq \frac{1}{|x|^n} + \frac{|p_1|}{|x|^{n-1}} + \cdots + \frac{|p_{n-1}|}{|x|} < \frac{n-1}{n} < 1,$$

luego

$$c = \frac{1}{x^n} + \frac{p_1}{x^{n-1}} + \cdots + \frac{p_{n-1}}{x} + 1 > 0,$$

y como $p_1^n(x) = x^n c$, la conclusión es inmediata. ■

2.3 Cuerpos formalmente reales

La *teoría de los cuerpos formalmente reales* es la teoría CFR sobre $\mathcal{L}_A^-$ determinada por los axiomas de C más el esquema axiomático[4]

FR *Para cada número natural $n \geq 1$:*

$$x_1^2 + \cdots + x_n^2 \neq -1.$$

Obviamente todas estas fórmulas son teoremas de CO. Observemos que en CFR se demuestra:

$$x_1^2 + \cdots + x_n^2 = 0 \to x_1 = \cdots = x_n = 0.$$

En efecto, si un $x_i \neq 0$, no perdemos generalidad si suponemos que es $x_n \neq 0$, y entonces

$$(x_1/x_n)^2 + \cdots + (x_{n-1}/x_n)^2 = -1.$$

Vamos a necesitar dos resultados sobre CFR:

Teorema 2.16 *Si $p_1^{2n+1}(x)$ es un polinomio irreducible de grado impar, y $k[\xi]$ es la adjunción a k de una de sus raíces, entonces $k[\xi]$ cumple* **FR**.

[4]En la teoría de conjuntos se demuestra que esta condición es equivalente a que exista una relación de orden con la que el cuerpo se convierta en un cuerpo ordenado, pero la prueba usa el axioma de elección (véase el teorema 7.59 de mi libro de álgebra).

DEMOSTRACIÓN: Supongamos que existen $\alpha_1, \ldots, \alpha_m \in k[\xi]$ tales que

$$\alpha_1^2 + \cdots + \alpha_m^2 = -1.$$

Recordando que $\alpha_i = \alpha_i(\xi)$, tenemos que ξ es raíz del polinomio

$$1 + \alpha_1(X)^2 + \cdots + \alpha_m(X)^2,$$

luego existe un polinomio $h(X)$ tal que

$$p_1^{2n+1}(X)h(X) = 1 + \alpha_1(X)^2 + \cdots + \alpha_m(X)^2. \qquad (*)$$

Cada $\alpha_i(X)$ tiene grado $\leq 2n$. Sea u el máximo de los grados de los $\alpha_i(X)$. Para cada i tal que $\operatorname{grad} \alpha_i(X) = u$, descomponemos $\alpha_i(X) = a_i X^u + g_i(X)$, donde $\operatorname{grad} g_i(X) < u$.

El coeficiente director del miembro derecho de $(*)$ es $\sum_i a_i^2$, donde i recorre únicamente los índices para los que $\operatorname{grad} \alpha_i(X) = u$. Aquí tenemos en cuenta que, como los a_i son no nulos, **FR** implica que la suma es no nula.

Por lo tanto, $p_1^{2n+1}(X)h(X)$ tiene grado $2u$, luego $h(X)$ tiene grado impar y tiene un factor irreducible $q(X)$ también de grado impar $2n' + 1 < 2n + 1$. Sea ζ una raíz de $q(X)$ (tal vez $\zeta \in k$ si $q(X)$ tiene grado 1). Al sustituir en $(*)$ obtenemos que -1 es suma de cuadrados en $k[\zeta]$.

A partir de aquí podemos repetir el proceso, y como cada vez pasamos de una extensión a otra menor, tras un número finito de pasos hemos de llegar a que $\zeta \in k$, con lo que tenemos una contradicción, porque -1 no es suma de cuadrados en k. ■

Teorema 2.17 *Sean $k[\xi_1]$ y $k[\xi_2]$ las adjunciones a k de raíces de los polinomios $X^2 + a$ y $X^2 - a$. Entonces, una de las dos es formalmente real.*

DEMOSTRACIÓN: Podemos suponer que ambos polinomios son irreducibles, pues en caso contrario una de las extensiones es k y la conclusión es trivial. Si -1 es suma de m cuadrados en $k[\xi_1]$, entonces

$$\sum_{i=1}^m (a_i + b_i\xi_1)^2 = \sum_{i=1}^m (a_i^2 - ab_i^2 + 2a_ib_i\xi_1) = -1,$$

y como $1, \xi_1$ forman una base de $k[\xi_1]$, de hecho

$$\sum_{i=1}^m (a_i^2 - ab_i^2) = -1.$$

Equivalentemente, $A + 1 = aB$, donde A y B son sumas de cuadrados en k (y el miembro izquierdo es no nulo, porque es una suma de cuadrados con un sumando no nulo, luego también $B \neq 0$). Similarmente, si -1 es suma de n cuadrados en $k[\xi_2]$ llegamos a que $C + 1 = -aD$, donde C y D son sumas de cuadrados en k, con $D \neq 0$.

Despejando a e igualando queda $BC + B + DA + D = 0$, pero es claro que los productos de sumas de cuadrados son sumas de cuadrados, luego tenemos una suma de cuadrados nula en k con sumandos no nulos, contradicción. ■

2.4 Cuerpos realmente cerrados

Introducimos ahora la clase de cuerpos ordenados que más se aproxima al concepto de "cuerpo de los números reales" que puede definirse en el seno de la lógica de primer orden. Existen distintos axiomas equivalentes (esquemas axiomáticos en realidad) que determinan los cuerpos realmente cerrados. El teorema siguiente recoge algunos de ellos (y en 2.44 veremos uno más):

Teorema 2.18 *Las afirmaciones siguientes son equivalentes:*[5]

1. *Para todo número natural n:*

$$u < v \wedge p^n(u)p^n(v) < 0 \rightarrow \bigvee d(u < d < v \wedge p^n(d) = 0),$$

2. $x \geq 0 \rightarrow \bigvee y\ x = y^2$,
   Para todo número natural n impar: $\bigvee x\ p^n(x) = 0$,

3. *Para todo número natural $n \geq 1$:* $\bigvee z \in C\ p^n(z) = 0$,

4. *Todo polinomio no constante en $C[X]$ tiene una raíz en C.*

5. *Todo polinomio irreducible en $C[X]$ tiene grado 1.*

6. *Todo polinomio irreducible en $R[X]$ tiene grado 1 o 2.*

DEMOSTRACIÓN: 1. $\Rightarrow$ 2. Si $a > 0$, entonces $p(X) = X^2 - a$ cumple que $p(0) = -a < 0$ y $p(a+1) = a^2 + a + 1 > 0$, luego 1. implica que existe un d tal que $d^2 - a = 0$. Para la segunda parte basta aplicar el teorema 2.15.

2. $\Rightarrow$ 3. Vamos a probar que si $p_1^n(X)$ es un polinomio mónico que en una extensión algebraica de R se escinde con todas sus raíces simples, entonces tiene una raíz en C. Expresamos $n = 2^m r$, con r impar y razonamos por inducción sobre m. Si $m = 0$ tenemos por hipótesis que el polinomio tiene una raíz en R, luego en particular en C.

Supongamos ahora que todo polinomio mónico de grado no divisible entre 2^m y que se escinde en una extensión algebraica de R con raíces simples tiene al menos una raíz en C y sea $p_1^n(X)$ un polinomio con $n = 2^m r$ tal que en una extensión $R[\theta]$, que podemos tomar normal, se escinde con todas sus raíces simples, digamos $\alpha_1, \ldots, \alpha_n$.

Observemos que si $1 \leq j < k \leq n$, $1 \leq j' < k' \leq n$ y los dos pares de índices (salvo el orden) no son los mismos, la ecuación

$$\alpha_j\alpha_k + x(\alpha_j + \alpha_k) = \alpha_{j'}\alpha_{k'} + x(\alpha_{j'} + \alpha_{k'})$$

tiene a lo sumo una solución.

[5]Notemos que cada apartado no es una fórmula, sino un esquema de infinitas fórmulas. Se trata de probar que si añadimos uno de ellos a CO como esquema axiomático, podemos probar los otros como esquemas teoremáticos.

En efecto, si $\alpha_j + \alpha_k \neq \alpha_{j'} + \alpha_{k'}$, podemos despejar x y la solución es única. Para que no sea así, tiene que ser $\alpha_j + \alpha_k = \alpha_{j'} + \alpha_{k'}$, en cuyo caso no habrá solución salvo que también $\alpha_j\alpha_k = \alpha_{j'}\alpha_{k'}$. Suponemos, pues, que se cumple

$$\alpha_j + \alpha_k = \alpha_{j'} + \alpha_{k'}, \qquad \alpha_j\alpha_k = \alpha_{j'}\alpha_{k'}.$$

Si $\alpha_j = 0$, tiene que ser $\alpha_{j'} = 0$ o bien $\alpha_{k'} = 0$, y en ambos casos se llega a que $\{\alpha_j, \alpha_k\} = \{\alpha_{j'}, \alpha_{k'}\}$. Por lo tanto, podemos suponer que $\alpha_j \neq 0$ y, razonando igualmente, que $\alpha_k \neq 0$, con lo que las cuatro raíces son no nulas. Entonces

$$\frac{\alpha_j}{\alpha_{j'}} = \frac{\alpha_{k'}}{\alpha_k} = \lambda.$$

Si $\lambda = 1$ tenemos que $\{\alpha_j, \alpha_k\} = \{\alpha_{j'}, \alpha_{k'}\}$, luego podemos suponer que $\lambda \neq 1$. Entonces $\lambda\alpha_{j'} + \alpha_k = \alpha_{j'} + \lambda\alpha_k$, luego $(\lambda - 1)\alpha_{j'} = (\lambda - 1)\alpha_k$, luego $\alpha_{j'} = \alpha_k$, de donde $\alpha_j = \alpha_{k'}$.

Así pues, en cualquier caso, se trata del mismo par de índices. Consecuentemente, como el número total de ecuaciones es $n(n-1)/2$ y R es infinito, podemos encontrar un $c \in R$ tal que los $n(n-1)/2$ números

$$\beta_{jk} = \alpha_j\alpha_k + c(\alpha_j + \alpha_k)$$

sean todos distintos dos a dos.

Ahora observamos que si aplicamos a β_{jk} una conjugación de $R[\theta]$, como ésta envía cada α_j a un $\alpha_{j'}$ y cada α_k a un $\alpha_{k'}$, obtenemos un $\beta_{j'k'}$. Eso significa que el polinomio mínimo de un β_{jk} es de la forma $(X - \beta^1) \cdots (X - \beta^u)$, donde los β^u son parte de los β_{jk}. Si no son todos, tomamos otro que no aparezca y razonamos igualmente: su polinomio mínimo será de esa forma, para otros β_{jk} diferentes (porque dos polinomios irreducibles de $R[X]$ no pueden tener raíces comunes en $R[\theta]$, ya que el polinomio mínimo de una raíz común debería dividir a ambos). Concluimos que

$$d(X) = \prod_{jk}(X - \beta_{jk}) \in R[X],$$

pues es un producto de polinomios mínimos de algunos β_{jk}, y es un polinomio que se escinde en $R[\theta]$ y cuyo grado es $n(n-1)/2$, no divisible entre 2^m. Por hipótesis de inducción tiene una raíz en C. No perdemos generalidad si suponemos que es $\alpha_1\alpha_2 + c(\alpha_1 + \alpha_2)$.

Ahora llamamos $\xi = \alpha_1\alpha_2$ y $\zeta = \alpha_1 + \alpha_2$. Según el teorema 1.47, existe un θ_0 tal que $R[\xi, \zeta] = R[\theta_0]$. Pongamos que esta extensión tiene grado d, de manera que θ_0 tiene d conjugados $\sigma(\theta_0)$. Pero si $\sigma(\theta_0) \neq \tau(\theta_0)$ entonces $\sigma(\xi + c\zeta) \neq \tau(\xi + c\zeta)$. En efecto, si $\sigma(\alpha_1) = \alpha_j$, $\sigma(\alpha_2) = \alpha_k$, $\tau(\alpha_1) = \alpha_{j'}$, $\tau(\alpha_2) = \alpha_{k'}$, entonces

$$\sigma(\xi + c\zeta) = \tau(\xi + c\zeta) \to \alpha_j\alpha_k + c(\alpha_j + \alpha_k) = \alpha_{j'}\alpha_{k'} + c(\alpha_{j'} + \alpha_{k'})$$

$$\to \{j, k\} = \{j', k'\} \to \sigma(\xi) = \tau(\xi) \land \sigma(\zeta) = \tau(\zeta) \to \sigma(\theta_0) = \tau(\theta_0).$$

Esto implica que $\xi + c\zeta$ tiene d conjugados distintos, por lo que las extensiones $R[\xi + c\zeta] \subset R[\xi, \zeta]$ tienen ambas el mismo grado, luego son iguales. En particular, $\xi, \zeta \in R[\xi + c\zeta] \subset C$.

Finalmente, el polinomio $(X - \alpha_1)(X - \alpha_2) = X^2 - \zeta + \xi \in C[X]$, luego tiene una raíz en C (las dos, realmente), luego $\alpha_1 \in C$, como había que probar.

En particular esto se aplica a cualquier polinomio mónico irreducible de $R[X]$, que tiene, por consiguiente, una raíz en C, y como todo polinomio de grado $n \geq 1$ tiene un factor mónico irreducible, también podemos afirmar que tiene una raíz en C.

3. $\Rightarrow$ 4. Basta tener en cuenta que $q(X) = p(X)\bar{p}(X) \in R[X]$, luego por 3. existe $z \in C$ tal que $p(z)\bar{p}(z) = 0$. Si es $\bar{p}(z) = 0$, aplicando la conjugación compleja, $p(\bar{z}) = 0$.

4. $\Leftrightarrow$ 5. Es inmediato, pues si un polinomio irreducible tiene una raíz, es que tiene grado 1 y si todo polinomio irreducible tiene grado 1, entonces todo polinomio no constante tiene un factor de grado 1, luego una raíz.

4. $\Rightarrow$ 6. Si $p(X) \in R[X]$ es irreducible y no tiene grado 1, entonces existe $z \in C$ tal que $p(z) = 0$, pero conjugando resulta que $p(\bar{z}) = 0$, luego el polinomio $q(Z) = (X - z)(X - \bar{z}) \in R[X]$ es el polinomio mínimo de z, luego divide a $p(X)$ en $R[X]$, luego es $p(X)$.

6. $\Rightarrow$ 1. El polinomio $p^n(X)$ se descompone en producto de irreducibles. Si cada uno de ellos tomara el mismo signo en u y en v, lo mismo le sucedería a $p^n(X)$, luego al menos un factor irreducible toma signos distintos en u y en v. Basta probar que éste tiene una raíz entre u y v o, equivalentemente, no perdemos generalidad si suponemos que $p^n(X)$ es mónico e irreducible. Por hipótesis su grado es 1 o 2. Si tiene grado 1 entonces $p_1^1(X) = x - d$, y es claro que $u < d < v$.

Si es $p^2(X) = X^2 + bX + c$, entonces

$$p_1^2(X) = \left(X + \frac{b}{2}\right)^2 - \frac{b^2 - 4c}{4}.$$

Si fuera $b^2 - 4c < 0$, entonces sería $\bigwedge x\, p^2(x) > 0$, luego $p_1^2(X)$ no podría tomar signos opuestos en a y en b, luego $b^2 - 4c \geq 0$. Por el teorema 2.11 tenemos que $p_1^2(X)$ tiene una raíz en R (luego, necesariamente, dos) y podemos factorizarlo

$$p_1^2(X) = (X - c_1)(X - c_2).$$

Es fácil ver que para que tome signos opuestos en u y en v es necesario que una de las raíces cumpla $u < c_i < v$. ■

La *teoría de los cuerpos realmente cerrados* es la teoría CRC que resulta de añadir a C como esquema axiomático cualquiera de los apartados del teorema anterior.

Observemos que, por el apartado 2., se cumple que CRC extiende a CE.

Teorema 2.19 *Si $q(X)$ es un polinomio, entonces la clase $A = \{x \mid q(x) > 0\}$ es una unión finita de intervalos.*

Demostración: Distinguimos dos casos: si $\bigwedge x\ q(x) \neq 0$, entonces se cumple que $A = \varnothing \lor A =]-\infty, +\infty[$. En efecto, en caso contrario existirían $x \in A$, $y \notin A$, de modo que $q(x) > 0$ y $q(y) < 0$, y el apartado 1. de 2.18 nos daría un c tal que $q(c) = 0$, contradicción.

Supongamos ahora que $\bigvee x\ q(x) = 0$. Podemos suponer que $q(X)$ no es el polinomio nulo, pues en ese caso $A = \varnothing$. Por la observación tras el teorema 1.28, existen $d_1, \ldots, d_n$ tales que

$$q(d_1) = 0 \land \cdots \land q(d_n) = 0 \land \bigwedge x(q(x) = 0 \to x = d_1 \lor \cdots \lor x = d_n).$$

Más aún, ahora podemos suponer que $d_1 < \cdots < d_n$. Llamamos $I_0 =]-\infty, d_0[$, $I_i =]d_i, d_{i+1}[$, $I_n =]d_n, +\infty[$. Es claro entonces que $A \subset I_0 \cup \cdots \cup I_n$. El apartado 1. de 2.18 implica claramente que

$$\bigwedge x \in I_i\ q(x) > 0 \lor \bigwedge x \in I_i\ q(x) < 0.$$

Equivalentemente, $I_i \subset A \lor I_i \cap A = \varnothing$. De aquí se concluye que A es la unión de los intervalos I_i que contiene. ■

Axiomatización alternativa de CRC Es interesante observar que CRC admite una axiomatización equivalente, a saber, la formada por los axiomas de C más los axiomas siguientes:

CRC1	$x^2 + y^2 \neq -1$
CRC2	$\bigvee y(x = y^2 \lor -x = y^2)$
CRC3	$\bigvee x\, p_1^n(x) = 0$ (para todo n impar)
CRC4	$x > 0 \leftrightarrow x \neq 0 \land \bigvee y\ x = y^2$

Ciertamente, todos ellos son teoremas de CRC. Sólo falta probar que a partir de ellos se demuestran los axiomas de CO y el axioma euclídeo **E**:

Para probar **CO1** suponemos que $x > 0 \land -x > 0$, que por **CRC4** implica que existen y, z no nulos tales que $x = y^2 = -z^2$, luego $(y/z)^2 + 0^2 = -1$, en contradicción con **CRC1**.

Es claro que **CRC2** y **CRC4** implican **CO2**.

Para probar **CO3** tomamos $x > 0 \land y > 0$, de modo que, por **CRC4** existen u, v no nulos tales que $x = u^2 \land y = v^2$. Por **CRC2**, o bien $u^2 + v^2 = w^2$, o bien $u^2 + v^2 = -w^2$. En el segundo caso, si suponemos $w \neq 0$, entonces $(u/w)^2 + (v/w)^2 = -1$, en contradicción con **CRC1**, luego es $w = 0$, pero entonces $(u/v)^2 + 0^2 = -1$, e igualmente tenemos una contradicción. Concluimos que $u^2 + v^2 = w^2$, con $w \neq 0$ por el mismo motivo, luego $x + y > 0$.

La prueba de **CO4** es inmediata, y **E** se sigue de **CRC4**. ■

Notemos que así es posible considerar a CRC como una teoría axiomática sobre $\mathcal{L}_A^-$ convirtiendo el axioma **CRC4** en una definición de $x > 0$.

Cuerpos algebraicamente cerrados Aunque no nos va a hacer falta, todos los resultados que vamos a probar para cuerpos realmente cerrados admiten versiones análogas (con demostraciones más sencillas) para la *teoría de los cuerpos algebraicamente cerrados,* que es la teoría CAC sobre el lenguaje $\mathcal{L}_A^-$ que resulta de añadir a C el esquema axiomático

AC *Para todo número natural* $n \geq 1$*:* $\bigvee x \; P_1^n(x) = 0$.

Observemos que CAC implica el esquema axiomático **Inf**. En efecto, supongamos que no se cumple su fórmula n-sima:

$$\bigvee x_1 \cdots x_{n+1} \bigwedge_{i \neq j} x_i \neq x_j$$

Es fácil ver que, reduciendo n si es preciso, podemos suponer que

$$\bigvee x_1 \cdots x_n \bigwedge_{i \neq j} x_i \neq x_j \wedge \bigwedge x_1 \cdots x_{n+1} \bigvee_{i \neq j} x_i = x_j,$$

de donde se sigue que

$$\bigvee x_1 \cdots x_n \bigwedge x (x = x_1 \vee \cdots \vee x = x_n),$$

pero entonces $(X - x_1) \cdots (X - x_n) + 1$ sería un polinomio mónico sin raíces, en contradicción con CAC.

Sin embargo, al contrario de lo que sucede con CRC, la teoría CAC no implica el esquema **Car0**, por lo que podemos considerar las extensiones CAC_0 y CAC_p que resultan de añadir a CAC el esquema axiomático **Car0** o el axioma **Car p**, para cada primo p.

Notemos que en CRC se prueba que el cuerpo C de los números complejos cumple los axiomas de CAC.

Análisis matemático en CRC No es posible formalizar el cálculo diferencial en CRC, pero aquí vamos a demostrar versiones algebraicas (para polinomios) de algunos teoremas clásicos del cálculo de una variable real: el teorema de Rolle, el teorema del valor medio y la relación entre derivadas y crecimiento de funciones.

Teorema 2.20

$$\bigwedge yz (y < z \wedge p(y) = p(z) = 0 \rightarrow \bigvee x (y < x < z \wedge f'(x) = 0)).$$

Demostración: No perdemos generalidad si suponemos que f no tiene raíces en $]y, z[$. Aplicando dos veces el teorema 1.27 podemos factorizar

$$p(X) = (X - y)^u (X - z)^v q(X),$$

donde $q(X)$ no se anula ni en y ni en z. Además $q(X)$ tampoco se anula en $]y, z[$, luego por la primera parte de 2.18 tiene signo constante en dicho intervalo. Ahora calculamos

$$p'(X) = (X - y)^{u-1} (X - z)^{v-1} h(X),$$

donde

$$h(X) = u(X-z)q(X) + v(X-y)q(X) + (X-y)(X-z)h'(X).$$

Entonces $h(y) = u(y-z)q(y)$ y $h(z) = v(z-y)q(z)$ tienen signos opuestos, luego existe un x tal que $y < x < z$ y $h(x) = 0$, luego también $f'(x) = 0$. ■

Teorema 2.21 $\bigvee c(a < c < b \land p(b) - p(a) = p'(c)(b-a))$.

DEMOSTRACIÓN: Sea $q(X) = p(X) - p(a) - \frac{p(b)-p(a)}{b-a}(x-a)$. Claramente $q(a) = 0 = q(b)$, luego por el teorema anterior existe $a < c < b$ tal que $q'(c) = 0$, pero

$$q'(X) = p'(X) - \frac{p(b)-p(a)}{b-a},$$

de donde se sigue inmediatamente la conclusión. ■

De aquí se sigue inmediatamente:

Teorema 2.22 $y < z \land \bigwedge x(y < x < z \to p'(x) > 0) \to p(y) < p(z)$.

2.5 La consistencia de CRC

Vamos a dar ahora una demostración completamente constructiva del teorema siguiente:

Teorema 2.23 *Si* CFR *es consistente, también lo es* CRC.

DEMOSTRACIÓN: Vamos a ver cómo transformar una demostración de $0 \neq 0$ en CRC en otra en CFR.

Sea $\bar{\mathcal{L}}_A$ el lenguaje formal que resulta de añadir a $\mathcal{L}_A^-$ dos funtores monádicos $(\ )^{-1}$ y r_2 y, para cada natural impar $n \geq 3$, un funtor $n-1$-ádico r_n. Llamaremos CRC* a la teoría axiomática sobre $\bar{\mathcal{L}}_A$ cuyos axiomas son los siguientes:

1. Los axiomas de C, salvo **C8**, que lo sustituimos por $0^{-1} = 0$ y
$$x \neq 0 \to x \cdot x^{-1} = 1,$$
2. **CRC1** $x^2 + y^2 \neq -1$,
3. **CRC2*** $x = r_1(x)^2 \lor -x = r_2(x)^2$,
4. **CRC3*** Para todo número natural impar $n \geq 3$,
$$p_0 + p_1 r_n(\bar{p}) + \cdots p_{n-1} r_n(\bar{p})^{n-1} + r_n(\bar{p})^n = 0,$$
5. Todas las fórmulas que resultan de sustituir variables libres por términos de $\bar{\mathcal{L}}_A$ en las fórmulas precedentes.

De este modo, los axiomas de CRC* son una familia de fórmulas sin cuantificadores cerrada para sustituciones de variables por términos. Además, definiendo $x > 0$ mediante **CRC4** es claro que todos los axiomas de CRC son demostrables en CRC*.

Por consiguiente, si tuviéramos una demostración de $0 \neq 0$ en CRC, a partir de ella podríamos construir una demostración de $0 \neq 0$ en CRC*.

Dicha demostración podría formalizarse igualmente en el cálculo secuencial LK, y podemos aplicar el teorema A20 de [LM],[6] según el cual sería posible demostrar $0 \neq 0$ con una demostración compuesta exclusivamente por fórmulas sin cuantificadores.

Es claro que si en dicha prueba sustituimos todas las variables libres por la constante 0, el resultado sigue siendo una demostración de $0 \neq 0$, puesto que los axiomas se transforman en axiomas y que cada una de las reglas de inferencia sigue siendo válida tras la sustitución (teniendo en cuenta que, como la prueba no tiene cuantificadores, en ella no se usan las reglas del particularizador). Así tenemos una demostración de $0 \neq 0$ sin cuantificadores ni variables libres.

Podemos ordenar todos los designadores que aparezcan en la prueba en una sucesión $t_1, \ldots, t_l$ de modo que si $i \leq l_0$ entonces t_i no contenga funtores r_n, mientras que si $l_0 + 1 \leq i \leq l$, entonces t_i se obtenga aplicando un funtor r_n a términos anteriores de la sucesión.

Una simple inducción prueba que $1 \leq i \leq l_0$, existen enteros u_i, v_i con $v_i \neq 0$ tales que en C se demuestra que $t_i = u_i \cdot v_i^{-1}$.

Sea $\bar{\mathcal{L}}_A^-$ el lenguaje formal que consta de los signos de $\mathcal{L}_A^-$ más l constantes $c_1, \ldots, c_l$. Definimos CFR* como la teoría axiomática sobre $\bar{\mathcal{L}}_A^-$ cuyos axiomas sean[7] los de CFR más un nuevo axioma para cada constante c_i:

- Si $1 \leq i \leq k$ tomamos como axioma $v_i c_i = u_i$.
- Si $t_i = e_2(t_j)$, con $j < i$, tomamos como axioma
$$c_i = c_j^2 \vee -c_i = c_j^2.$$
- Si $t_i = e_n(t_{j_0}, \ldots, t_{j_{n-1}})$, con n impar y $j_0, \ldots, j_{n-1} < i$, tomamos como axioma
$$c_{j_0} + c_{j_1} c_i + \cdots c_{j_{n-1}} c_i^{n-1} + c_i^n = 0.$$

Una simple inducción muestra que la prueba que estamos considerando sobre CRC* se convierte en una prueba de $0 \neq 0$ en CFR* si sustituimos cada término t_i por la constante c_i. (No es que el resultado de la sustitución sea ya de por sí una prueba, pero en cada paso se pueden intercalar los pasos oportunos para que lo sea).

Ahora vamos a definir en CFR una interpretación de CFR*, con lo que concluiremos que CFR es contradictoria.

[6] Mi libro de Lógica Matemática.

[7] En realidad sólo necesitamos incluir en CFR* el caso $x^2 + y^2 \neq -1$ del esquema **FR**.

Concretamente, vamos a definir recurrentemente un árbol de extensiones algebraicas de R de altura $l - l_0$. Para empezar asignamos a cada constante c_i, con $1 \leq i \leq l_0$ el designador (definido) de $\mathcal{L}_A^-$

$$\bar{c}_i = u_i/v_i.$$

Si la constante c_{l_0} se ha introducido en CFR* con un axioma de la forma $c_{j_0} + c_{j_1}c_i + \cdots c_{j_{n-1}}c_i^{n-1} + c_i^n = 0$, consideramos el polinomio

$$\bar{c}_0 + \bar{c}_1 X + \cdots + \bar{c}_{n-1}X^{n-1} + X^n,$$

y tomamos un factor irreducible de grado impar. Si tiene grado 1 será de la forma $X - a$, para cierto $a \in R$, y definimos $\bar{c}_{l_0+1} = a$. Si tiene grado mayor que 1, tomamos una raíz ξ en una extensión algebraica y definimos $\bar{c}_{l_0+1} = \xi$. El nivel 1 del árbol está formado entonces por R o $R[\xi]$, según el caso, y en ambos se cumple que

$$\bar{c}_0 + \bar{c}_1\bar{c}_{l_0+1} + \cdots + \bar{c}_{n-1}\bar{c}_{l_0+1}^{n-1} + \bar{c}_{l_0+1}^n.$$

Por el contrario, si c_{l_0} se ha introducido en CFR* con un axioma de la forma $c_i = c_j^2 \vee -c_i = c_j^2$, consideramos los polinomios $X^2 \pm \bar{c}_j$. Si uno de los dos tiene una raíz $a \in R$, definimos $\bar{c}_{l_0+1} = a$ y tomamos R como la única extensión de nivel 1. Si por el contrario ambos polinomios son irreducibles, en el nivel 1 consideramos dos extensiones, $R[\xi_1]$ y $R[\xi_2]$, resultantes de adjuntar una raíz de cada uno de los polinomios, y definimos $\bar{c}_{l_0+1} = \xi_i$ en cada extensión (de modo que no hay un único $\bar{c}_{l_0+1}$, sino uno para cada extensión de nivel 1). En cualquier caso se cumple

$$\bar{c}_{l_0+1} = \bar{c}_j^2 \vee \bar{c}_{l_0+1} = -\bar{c}_j^2.$$

La construcción continúa del mismo modo: cada vez que c_{l_0+i} se introduce en CFR* como raíz de un polinomio de grado impar, cada extensión del nivel i-ésimo se extiende a una única extensión del nivel superior que puede ser la misma del nivel i-ésimo o bien una extensión de grado impar, y en cualquier caso se interpreta $\bar{c}_i$ en dicha extensión de modo que es una raíz del polinomio que resulta de sustituir las constantes c_j de $\bar{\mathcal{L}}_A^-$ por los términos (o multitérminos) $\bar{c}_j$ de $\mathcal{L}_A^-$. Por el contrario, si c_{l_0+i} se introduce en CFR* como una raíz cuadrada, cada extensión del nivel i-ésimo se extiende a una única extensión si dicha raíz cuadrada puede tomarse ya en la extensión de partida, o a dos extensiones distintas en caso contrario (puede ocurrir que dos extensiones del mismo nivel se encuentren en casos distintos). En caso de ramificación, el término (o multitérmino) $\bar{c}_i$ se define de forma distinta en cada una de las extensiones del nivel siguiente.

Tras un $l - l_0$ pasos llegamos a un número finito de extensiones algebraicas $K_1, \ldots K_N$ de R, cada una de las cuales se obtiene a partir de R mediante una sucesión de extensiones de grado 2 o de grado impar. Ahora, los teoremas 2.16 y 2.17 implican que al menos una de las extensiones K_i cumple $x^2 + y^2 \neq -1$. En efecto si suponemos que -1 es suma de dos cuadrados en cada una de ellas,

dichos teoremas nos dan que -1 es suma de cuadrados en cada extensión del nivel anterior, y descendiendo así en el árbol llegamos a que lo mismo sucede en R, en contradicción con los axiomas de CFR que estamos suponiendo.

Fijada una extensión K en la que -1 no sea suma de dos cuadrados, tenemos interpretaciones en K de las constantes $c_0, \ldots, c_l$, que satisfacen los axiomas que las introducen en CFR*, de modo que si en la prueba de $0 \neq 0$ en CFR* cambiamos cada constante c_i por $\bar{c}_i$, obtenemos una demostración en CFR de que el 0^* de K es distinto del 0^* de K, pero esto es una contradicción en CFR.

■

Sabemos que en CRC se prueba que $R[i]$ cumple los axiomas de CAC, por lo que una demostración de $0 \neq 0$ en CAC permite construir una demostración de $0^* \neq 0^*$ en CRC, donde 0^* es el $0 = (0,0)$ de $R[i]$. Así pues, si CAC es contradictorio, CRC también lo es.

Alternativamente, podemos repetir con CAC todo el proceso que hemos seguido con CRC en la prueba del teorema anterior, con la diferencia de que ahora omitimos todo lo relacionado con **CRC1** y **CRC2**. Ahora no tenemos que ramificar extensiones para preservar **FR**, sino que simplemente construimos una cadena de extensiones de k hasta obtener una extensión algebraica en la que existan raíces de todos los polinomios cuyas raíces se han usado en la supuesta prueba de $0 \neq 0$. El resultado es:

Teorema 2.24 *Si* C *es consistente, entonces* CAC *también lo es.*

Más precisamente, una ligera modificación de la prueba nos da la consistencia de CAC$_0$ y CAC$_p$ a partir de la de C$_0$ o C$_p$, respectivamente.

Por último, observemos que la consistencia de CFR es incuestionable, pues admite como modelo al cuerpo $\mathbb{Q}$ de los números racionales, el cual sirve igualmente de modelo de C$_0$, mientras que es posible definir explícitamente cuerpos finitos de cualquier característica prima p, que sirven como modelos de C$_p$ y prueban su consistencia.

2.6 Eliminación de cuantificadores

En esta sección demostraremos que CRC es una teoría axiomática completa, es decir, que cualquier sentencia de $\mathcal{L}_A$ es demostrable o refutable en CRC. Para ello nos demostraremos una propiedad notable, y es que toda fórmula de $\mathcal{L}_A$ es equivalente en CRC a otra fórmula sin cuantificadores con las mismas variables libres.[8]

Observemos en primer lugar que para ello basta probar que si $\phi(x, x_1, \ldots, x_n)$ es una fórmula sin cuantificadores, entonces existe otra fórmula $\psi(x_1, \ldots, x_n)$, también sin cuantificadores, tal que

$$\vdash_{\mathrm{CRC}} \bigvee x\, \phi(x, x_1, \ldots, x_n) \leftrightarrow \psi(x_1, \ldots, x_n).$$

[8] Siempre que hablemos de equivalencia entre fórmulas se entenderá que ambas tienen las mismas variables libres.

En efecto, si se cumple esto, lo mismo vale para $\bigwedge x\, \phi(x, x_1, \ldots, x_n)$, pues

$$\bigwedge x\, \phi(x, x_1, \ldots, x_n) \leftrightarrow \neg \bigvee x \neg \phi(x, x_1, \ldots, x_n) \leftrightarrow \neg \psi'(x_1, \ldots, x_n),$$

donde ψ' es una fórmula sin cuantificadores equivalente a $\bigvee x \neg \phi$.

A su vez, como toda fórmula puede ponerse en forma prenexa (es decir, como una sucesión de cuantificadores seguida de una fórmula sin cuantificadores), basta aplicar sucesivamente los dos casos anteriores para eliminar todos los cuantificadores.

El siguiente teorema general nos permite reducir aún más el problema:

Teorema 2.25 *Toda fórmula sin cuantificadores de un lenguaje formal es lógicamente equivalente a una de la forma* $\alpha_1 \lor \cdots \lor \alpha_k$, *donde cada* α_i *es de la forma* $\beta_{i1} \land \cdots \land \beta_{i,r_i}$, *y donde a su vez cada* β_{ij} *es una fórmula atómica o la negación de una fórmula atómica.*

Demostración: Hay que entender que las conjunciones y disyunciones que aparecen en el enunciado pueden reducirse a una sola fórmula. Vamos a probar, más en general, que toda fórmula y su negación son equivalentes tanto a una disyunción de conjunciones de fórmulas atómicas o sus negaciones como a una conjunción de disyunciones de tales fórmulas. Lo hacemos por inducción sobre la longitud de la fórmula.

Obviamente, toda fórmula atómica y su negación tienen ya la forma requerida. Si α es equivalente a una disyunción de conjunciones y a una conjunción de disyunciones, es claro que $\neg\alpha$ cumple lo mismo (por las leyes de De Morgan). Si α y β admiten tales equivalencias, entonces $\alpha \rightarrow \beta$ es equivalente a $\neg\alpha \lor \beta$, que claramente es equivalente a una disyunción de conjunciones y, usando que tanto $\neg\alpha$ como β son equivalentes a conjunciones de disyunciones, usando la propiedad distributiva se concluye sin dificultad que $\neg\alpha \lor \beta$ también es equivalente a una conjunción de disyunciones. ■

Para particularizar este teorema al caso de $\mathcal{L}_A$ y CO conviene introducir algunos conceptos:

Definición 2.26 Llamaremos *polinomios* en la variable x a los términos[9] de $\mathcal{L}_A$ de la forma $t_0 + t_1 x + \cdots + t_k x^k$, donde $t_0, \ldots, t_k$ son términos que no contienen la variable x. El número k se llama *grado* del polinomio y t_k es el *coeficiente director* del polinomio.

Una *fórmula elemental* (respecto de la variable x) de $\mathcal{L}_A$ es una fórmula

$$p_1 = 0 \land \cdots \land p_k = 0 \land q_1 > 0 \land \cdots \land q_l > 0,$$

donde los p_i, q_j son polinomios en la variable x.

[9] Observemos que esta noción de polinomio es puramente sintáctica, y no se corresponde con el concepto informal de polinomio que estábamos considerando hasta ahora.

El teorema siguiente se demuestra sin dificultad por inducción sobre la longitud de un término:

Teorema 2.27 *Si x es una variable, para cada término t de $\mathcal{L}_A$ existe un polinomio p en x tal que* $\vdash_{\mathrm{C}} t = p$.

Ahora particularizamos el teorema 2.25 al caso de CO:

Teorema 2.28 *Fijada una variable x, toda fórmula sin cuantificadores de $\mathcal{L}_A$ es equivalente en* CO *a una disyunción de fórmulas elementales.*

Demostración: Por el teorema 2.25, toda fórmula sin cuantificadores es equivalente a una disyunción de conjunciones de fórmulas atómicas y sus negaciones. Las fórmulas atómicas de $\mathcal{L}_A$ son de la forma $t_1 = t_2$ (que equivale a $t_1 - t_2 = 0$) y $t > 0$. La negación de una fórmula $t = 0$ es equivalente a $t > 0 \lor -t > 0$, y la de $t > 0$ es equivalente a $-t > 0 \lor t = 0$. Al hacer estas sustituciones en una conjunción de fórmulas elementales y negaciones, las disyunciones que introducimos pueden distribuirse, y el resultado es una conjunción de fórmulas atómicas de tipo $t = 0$ o $t > 0$. Según el teorema anterior, los términos pueden sustituirse por polinomios, con lo que obtenemos una disyunción de fórmulas elementales. ■

Así pues, para probar que toda fórmula de CRC es equivalente a una fórmula sin cuantificadores con las mismas variables libres basta probarlo para fórmulas de tipo $\bigvee x\,(\alpha_1 \lor \cdots \lor \alpha_m)$, donde cada α_i es una fórmula elemental, pero como esto equivale a $\bigvee x\,\alpha_1 \lor \cdots \lor \bigvee x\,\alpha_m$, en realidad basta probarlo para fórmulas de tipo

$$\bigvee x\,(p_1 = 0 \land \cdots \land p_k = 0 \land q_1 > 0 \land \cdots \land q_l > 0).$$

Observemos ahora que, con la definición sintáctica de polinomio que hemos introducido en este apartado, un término como $4+x-2x^2+0x^3$ es un polinomio de grado 3. Más en general, un polinomio como $4 + x - 2x^2 + (a - b)x^3$ tiene grado 3, aunque "su grado de verdad" puede ser 2 o 3 según si $a = b$ o $a \neq b$, pero esta distinción no tiene sentido metamatemáticamente, pues a y b no son más que dos variables de $\mathcal{L}_A$. Para evitar los inconvenientes que este hecho puede ocasionar introducimos el concepto siguiente:

Definición 2.29 Una fórmula en forma *cuasimónica* (en la variable x) es una fórmula $c \neq 0 \land \alpha$, donde α es una fórmula elemental respecto de x y c es un término sin la variable x de la forma $c = t_1 \cdots t_m$, donde entre los factores están todos los coeficientes directores de los polinomios de grado no nulo que intervienen en α.

Teorema 2.30 *Toda fórmula sin cuantificadores es equivalente en* CO *a una disyunción de fórmulas en forma cuasimónica.*

Demostración: Basta probarlo para fórmulas elementales $\alpha(x)$. Razonamos por inducción sobre el número k de monomios tx^i con $i > 0$ que aparecen en $\alpha(x)$. Si $k = 0$ es que todos los polinomios que aparecen en α tienen grado nulo, luego $1 \neq 0 \land \alpha$ está en forma cuasimónica y es equivalente a α.

Supongamos que el resultado es cierto para fórmulas con menos de k monomios de grado no nulo y sea $\alpha(x)$ una fórmula elemental con k monomios de grado no nulo. Sean $h_1, \ldots, h_m$ los polinomios de grado no nulo que aparecen en ella y sea c_i el coeficiente director de h_i. Entonces $\alpha(x)$ es equivalente a

$$(c_1 = 0 \land \alpha(x)) \lor (c_1 \neq 0 \land \alpha(x)).$$

La primera parte es equivalente a $c_1 = 0 \land \alpha'(x)$, donde α' es la fórmula que resulta de eliminar el monomio de mayor grado de $h_1(x)$. Así tenemos una fórmula elemental con $k-1$ monomios de grado no nulo (y un polinomio más de grado nulo), luego por hipótesis de inducción es equivalente a una disyunción de fórmulas en forma cuasimónica.

Si $m = 1$, la segunda parte ya está en forma cuasimónica, y en caso contrario es equivalente a

$$(c_2 = 0 \land c_1 \neq 0 \land \alpha(x)) \lor (c_1c_2 \neq 0 \land \alpha(x)).$$

Nuevamente, la primera parte es equivalente a $c_1 \neq 0 \land c_2 = 0 \land \alpha'(x)$, donde α' resulta de suprimir el término de mayor grado de h_2. Por hipótesis de inducción $c_2 = 0 \land \alpha'(x)$ es equivalente a una disyunción de fórmulas de tipo $c \neq 0 \land \gamma(x)$ en forma cuasimónica, con lo que $c_1 \neq 0 \land c_2 = 0 \land \alpha'(x)$ es equivalente a la disyunción de las fórmulas $c_1c_2 \neq 0 \land \gamma(x)$, que también están en forma cuasimónica.

La parte $c_1c_2 \neq 0 \land \alpha(x)$, o bien está ya en forma cuasimónica (si $m = 2$), o bien podemos repetir el proceso y, tras m pasos, el teorema queda probado. ■

Observemos que en la fórmula obtenida en la demostración del teorema anterior todos los polinomios que aparecen tienen grado menor o igual que polinomios de la fórmula de partida.

Vamos a probar por inducción sobre n la afirmación siguiente:

H(n) *Sea $\alpha(x)$ una fórmula sin cuantificadores, sea f un polinomio de grado $\leq n$ en la variable x, sea c un término que no contenga la variable x y que sea un producto entre cuyos factores se encuentre el coeficiente director de f. Entonces la fórmula*

$$\bigvee x(c \neq 0 \land f = 0 \land \alpha(x))$$

es equivalente en CRC *a una fórmula sin cuantificadores.*

Observemos que $H(0)$ es trivialmente cierta, pues si f es un polinomio de grado 0 y aparece como factor de c, la conjunción $c \neq 0 \land f = 0$ es contradictoria, luego la fórmula es equivalente, por ejemplo, a $0 > 0$. Suponemos $H(n)$ y demostraremos $H(n+1)$, para lo cual necesitaremos algunos teoremas previos.

Teorema 2.31 *Si f es un polinomio de grado $d \geq 1$ en la variable x, sea a su coeficiente director y sea g un polinomio de grado $m \geq d$. Entonces existen polinomios q y r, con r de grado menor que d, tales que en* C *se prueba que $a^{m-d+1}g = fq + r$.*

Demostración: Razonamos por inducción sobre $m-d$. Observemos que, si b es el coeficiente director de g, el polinomio $g_1 = ag - bx^{m-d}f$ tiene grado $m' < m$. Si $m-d=0$ basta tomar $r = g_1$. En caso contrario, si $m' < d$ tenemos que $a^{m-d+1}g = a^{m-d}fbx^{m-d} + a^{m-d}g_1$ y esta descomposición cumple el teorema. Si $d \leq m'$ aplicamos la hipótesis de inducción, que nos da

$$a^{m'-d+1}g_1 = fq' + r',$$

donde r' tiene grado menor que d. Por lo tanto

$$a^{m'-d+2}g = fba^{m'-d+1}x^{m-d} + a^{m'-d+1}g_1 = fba^{m'-d+1}x^{m-d} + fq' + r',$$

luego

$$a^{m-d+1}g = a^{m-m'-1}a^{m'-d+2}g =$$
$$fa^{m-m'-1}(ba^{m'-d+1}x^{m-d} + q') + a^{m-m'-1}r',$$

y también se cumple lo pedido. ■

Teorema 2.32 *Toda fórmula* $\bigvee x(c \neq 0 \land f = 0 \land \alpha(x))$ *en las condiciones de* $H(n)$ *con* α *elemental y* f *de grado no nulo es equivalente en* CO *a otra en la que todos los polinomios que aparecen en* $\alpha(x)$ *tienen grado menor que el grado de* f.

Demostración: Sea a el coeficiente director de f. Si $h(x)$ es uno de los polinomios que aparecen en $\alpha(x)$, podemos reemplazarlo por $a^N h(x)$ para cualquier N par, pues, bajo la hipótesis $c \neq 0$, que implica $a \neq 0$, las fórmulas $h(x) = 0$ o $h(x) > 0$ son equivalentes a $a^N h(x) = 0$ y $a^N h(x) > 0$, respectivamente. Concretamente, tomamos un N mayor que el grado de f, y así el teorema anterior nos da una descomposición $a^N h = fq + r$, donde el grado de r es menor que el de f y, bajo la hipótesis $f = 0$, resulta que $a^N h(x) = 0$ y $a^N h(x) > 0$ son equivalentes a $r(x) = 0$ y $r(x) > 0$, respectivamente. Sustituyendo cada $h(x)$ por el $r(x)$ correspondiente obtenemos una fórmula equivalente a la dada en las condiciones requeridas. ■

Teorema 2.33 *Supongamos* $H(n)$ *y que toda fórmula de tipo*

$$\bigvee x(c \neq 0 \land f = 0 \land q_1 > 0 \land \cdots \land q_l > 0)$$

(donde el grado de f *es* $n+1$*, todos los* q_j *tienen grado no nulo* $\leq n$ *y* c *es un producto sin la variable* x *entre cuyos factores se encuentran el coeficiente director de* f *y los de todos los polinomios* q_j*) es equivalente en* CRC *a una fórmula sin cuantificadores. Entonces se cumple* $H(n+1)$.

Demostración: Tomamos una fórmula de tipo $\bigvee x(c \neq 0 \land f = 0 \land \alpha(x))$ en las condiciones de $H(n+1)$. Si el grado de f es $\leq n$, entonces podemos aplicar $H(n)$ a la fórmula dada para concluir que es equivalente a una fórmula sin cuantificadores. Podemos suponer, pues, que f tiene grado $n+1$.

Por 2.28 podemos suponer que α es una disyunción de fórmulas elementales y la fórmula dada es equivalente a las disyunciones correspondientes, por lo que no perdemos generalidad si suponemos que $\alpha(x)$ es elemental. Por el teorema anterior podemos suponer que todos los polinomios que aparecen en $\alpha(x)$ tienen grado $\leq n$ y por 2.30 $\alpha(x)$ es equivalente a una disyunción de fórmulas cuasimónicas (cuyos polinomios siguen teniendo grado $\leq n$, según la observación posterior a dicho teorema). Por lo tanto, no perdemos generalidad si consideramos fórmulas de tipo

$$\bigvee x(c \neq 0 \wedge c' \neq 0 \wedge f = 0 \wedge p_1 = 0 \wedge \cdots \wedge p_k = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0),$$

donde c' es un producto entre cuyos factores están todos los coeficientes directores de los polinomios p_i, q_j de grado no nulo. Tenemos que probar que cada una de estas fórmulas es equivalente a una fórmula sin cuantificadores. En realidad, como las subfórmulas con polinomios de grado nulo se pueden extraer del cuantificador, podemos suponer que todos los polinomios p_i, q_j tienen grado no nulo Si cambiamos c por cc', nos queda

$$\bigvee x(c \neq 0 \wedge f = 0 \wedge p_1 = 0 \wedge \cdots \wedge p_k = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0),$$

donde ahora c es un producto divisible entre el coeficiente director de f y los de todos los polinomios p_i, q_j.

Si $k > 0$ podemos aplicar $H(n)$ a esta fórmula tomando como la f de $H(n)$ el polinomio p_1 (y considerando a la f de la fórmula que tenemos como parte de la $\alpha(x)$ de $H(n)$). Si $k = 0$ la conclusión se tiene por la hipótesis de este teorema, que es, por lo tanto, lo único que nos falta probar para demostrar $H(n+1)$. ■

El teorema siguiente termina de perfilar la estructura global de la prueba:

Teorema 2.34 *Si se cumple $H(n)$ para todos los números naturales y toda fórmula de tipo*

$$\bigvee x(c \neq 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0)$$

(donde c es un producto sin la variable x entre cuyos factores están los coeficientes directores de los polinomios q_j, todos los cuales tienen grado no nulo) es equivalente en CRC *a una fórmula sin cuantificadores, entonces toda fórmula de $\mathcal{L}_R$ es equivalente en* CRC *a otra fórmula sin cuantificadores.*

Demostración: Al principio de este apartado ya hemos razonado que basta probarlo para fórmulas de tipo $\bigvee x\, \alpha(x)$, donde $\alpha(x)$ no tiene cuantificadores. Por 2.30 podemos suponer que $\alpha(x)$ está en forma cuasimónica, extrayendo del particularizador las conjunciones correspondientes a polinomios de grado nulo nos reducimos al caso de una fórmula de tipo

$$\bigvee x(c \neq 0 \wedge p_1 = 0 \wedge \cdots \wedge p_k = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0),$$

donde c es un producto que no contiene la variable x entre cuyos factores están los coeficientes directores de todos los polinomios p_i, q_j. Si $k \neq 0$ y p_1 tiene grado n basta aplicar $H(n)$ con $f = p_1$, mientras que si $k = 0$ la conclusión se sigue de la hipótesis de este teorema. ■

Ahora probamos algunos resultados concretos sobre eliminación de cuantificadores:

Teorema 2.35 *Supongamos que se cumple $H(n)$, sea $g(x)$ un polinomio de grado $\leq n$ y sea c un producto de términos sin la variable x entre cuyos factores esté el coeficiente director de g. Sean y, z dos variables que no aparezcan en g ni en c. Entonces las fórmulas siguientes son equivalentes en* CRC *a fórmulas sin cuantificadores:*

1. $c \neq 0 \wedge y < z \wedge \bigwedge x(y < x < z \rightarrow g(x) \neq 0)$,
2. $c \neq 0 \wedge \bigwedge x(y < x \rightarrow g(x) \neq 0)$,
3. $c \neq 0 \wedge \bigwedge x(x < z \rightarrow g(x) \neq 0)$,
4. $c \neq 0 \wedge \bigwedge x\ g(x) \neq 0$.

Demostración: En todos los casos podemos suponer que g tiene grado no nulo, pues en otro caso la fórmula con el generalizador puede sustituirse simplemente por $g \neq 0$.

1. es equivalente a

$$c \neq 0 \wedge y < z \wedge \neg \bigvee x(c \neq 0 \wedge g(x) = 0 \wedge x - y > 0 \wedge z - x > 0),$$

y podemos aplicar $H(n)$ a la fórmula con el particularizador. Los otros casos se prueban de forma similar. ■

Teorema 2.36 *Sea $f(x)$ un polinomio y sea c un producto sin la variable x entre cuyos factores figure el coeficiente director de f. Entonces las fórmulas siguientes son equivalentes en* CO *a fórmulas sin cuantificadores:*

1. $c \neq 0 \wedge \bigvee M \bigwedge x(x > M \rightarrow f(x) > 0)$,
2. $c \neq 0 \wedge \bigvee M \bigwedge x(x < M \rightarrow f(x) < 0)$.

Demostración: El teorema 2.15 muestra que si f tiene grado n y a es su coeficiente director, entonces 1. es equivalente a $c \neq 0 \wedge a > 0$, mientras que 2. es equivalente a $(-1)^{n+1}a > 0$. ■

Teorema 2.37 *Consideremos una fórmula de tipo*

$$\bigvee x(c \neq 0 \wedge f = 0 \wedge q_0 > 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0),$$

donde[10] *$q_0 = f'$ y c es un producto sin la variable x entre cuyos factores se encuentran el coeficiente director de f y los de todos los polinomios q_k. Entonces dicha fórmula es equivalente en* CRC *a la disyunción de las fórmulas siguientes (para i, $j = 0, \ldots, l$), donde n_k es el grado de q_k:*

[10] La derivada de un polinomio se define análogamente a 1.36.

$\mathbf{A_{i,j}}$ $c \neq 0 \land \bigvee yz(y < z \land f(y) < 0 \land f(z) > 0 \land q_i(y) = 0 \land q_j(z) = 0 \land$

$$\bigwedge_{k=0}^{l} (\bigwedge x(y < x < z \to q_k(x) \neq 0)) \land \bigwedge_{k=0}^{l} \bigvee_{r=0}^{n_k} (q_k^{r)}(y) > 0 \land \bigwedge_{u=1}^{r-1} q_k^{u)}(y) = 0),$$

$\mathbf{B_j}$ $c \neq 0 \land \bigvee y(q_j(y) = 0 \land f(y) < 0 \land \bigvee M \bigwedge v > M \ f(v) > 0 \land$

$$\bigwedge_{k=0}^{l} (\bigwedge x(y < x \to q_k(x) \neq 0)) \land \bigwedge_{k=0}^{l} q_k(y+1) > 0),$$

$\mathbf{C_j}$ $c \neq 0 \land \bigvee z(q_j(z) = 0 \land f(z) > 0 \land \bigvee M \bigwedge u < M \ f(u) < 0 \land$

$$\bigwedge_{k=0}^{l} (\bigwedge x(x < z \to q_k(x) \neq 0)) \land \bigwedge_{k=0}^{l} q_k(z-1) > 0),$$

D $c \neq 0 \land \bigvee M \bigwedge u < M \ f(u) < 0 \land \bigvee M \bigwedge v > M \ f(v) > 0 \land$

$$\bigwedge_{k=0}^{l} (\bigwedge x \ q_k(x) \neq 0) \land \bigwedge_{k=1}^{l} q_k(0) > 0).$$

DEMOSTRACIÓN: Si se cumple A_{ij}, tenemos que f toma signos opuestos en los extremos del intervalo $]y, z[$, luego por la primera parte del teorema 2.18 tenemos que existe un x en el intervalo donde $f(x) = 0$. Por otra parte sabemos que los q_k no se anulan en el intervalo, luego por el mismo motivo no cambian de signo. La última parte de A_{ij} afirma que cada la menor derivada no nula de cada q_k en y es positiva, lo cual, según el teorema 2.14, implica que q_k es positivo en los puntos situados a la derecha de y, luego en todo el intervalo $]y, z[$, y en particular en x.

La demostración de que cada una de las fórmulas B_j, C_j y D implican la fórmula inicial es similar.

Supongamos ahora que un cierto x cumple la fórmula dada. Distinguimos dos casos, según si alguno de los polinomios q_k tiene al menos una raíz o el caso contrario. Trataremos el primero y dejamos al lector el segundo, para el que el razonamiento necesario es una simplificación del que vamos a ver (y conduce a que se cumple D). Usando la observación tras el teorema 1.28 concluimos que existen $a_1 < \cdots < a_N$ tales que en cada a_i se anula un q_k y toda raíz de un q_k es alguno de los a_r.

Notemos que x no puede ser igual a ninguno de los a_i, porque todos los g_k son positivos en x. Esto nos da que $x < a_1$, o bien $x > a_N$ o bien $a_i < x < a_{i+1}$ para algún i. Vamos a suponer que se da el último caso y dejamos al lector el análisis de los otros tres.

Si llamamos $y = a_i$, $z = a_{i+1}$, es claro que se cumple todo lo que A_{ij} exige sobre las q_k (la primera derivada no nula de cada q_k en y tiene que ser positiva porque q_k tiene signo constante en $]y, z[$ y es positiva en x). Falta probar que $f(y) < 0$ y $f(z) > 0$. Ahora bien, como $g_0 = f'$ es positiva en $]y, z[$, el teorema 2.22 nos da que $f(y) < f(x) = 0 < f(z)$. ■

Teorema 2.38 *Se cumple $H(n)$ para todo número natural n.*

DEMOSTRACIÓN: Suponemos $H(n)$ y, según el teorema 2.33, basta probar que toda fórmula

$$\bigvee x(c \neq 0 \wedge f = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0)$$

en las condiciones de su enunciado es equivalente a una fórmula sin cuantificadores. Llamamos $g_0 = f'$ y descomponemos la fórmula dada en la disyunción de las tres fórmulas

$$\bigvee x(c \neq 0 \wedge g_0 = 0 \wedge f = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0),$$

$$\bigvee x(c \neq 0 \wedge f = 0 \wedge g_0 > 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0),$$

$$\bigvee x(c \neq 0 \wedge f = 0 \wedge -g_0 > 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0).$$

La primera es equivalente a una fórmula sin cuantificadores por $H(n)$, ya que g_0 tiene grado n. La tercera se reduce a la segunda cambiando f por $-f$, luego basta probar que la segunda es equivalente a una fórmula sin cuantificadores. Por el teorema anterior basta ver que esto ocurre con todas las fórmulas A_{ij}, B_j, C_j y D. Consideremos el caso de A_{ij}. Por 2.35 sabemos que las fórmulas

$$\bigwedge x(y < x < z \rightarrow q_k(x) \neq 0)$$

son equivalentes a fórmulas sin cuantificadores. Al sustituirlas por tales equivalentes, obtenemos una fórmula de tipo

$$\bigvee y(c \neq 0 \wedge q_i(y) = 0 \wedge \bigvee z(c \neq 0 \wedge q_j(z) = 0 \wedge \beta)),$$

donde β no tiene cuantificadores. Podemos aplicar $H(n)$ a la fórmula que empieza por $\bigvee z$ para sustituirla por una fórmula sin cuantificadores, y a continuación hacer lo mismo con la fórmula completa resultante.

Los otros casos se razonan análogamente. ■

Omitimos la prueba del teorema siguiente, pues resulta de simplificar la del teorema 2.37:

Teorema 2.39 *Consideremos una fórmula de tipo*

$$\bigvee x(c \neq 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0),$$

donde c es un producto sin la variable x entre cuyos factores se encuentran el coeficiente director de f y los de todos los polinomios q_k. Entonces dicha fórmula es equivalente en CRC *a la disyunción de las fórmulas siguientes (para i, $j = 1, \ldots, l$), donde n_k es el grado de q_k:*

$\mathbf{A_{i,j}}$ $c \neq 0 \wedge \bigvee yz(y < z \wedge q_i(y) = 0 \wedge q_j(z) = 0 \wedge$

$$\bigwedge_{k=1}^{l} (\bigwedge x(y < x < z \rightarrow q_k(x) \neq 0)) \wedge \bigwedge_{k=1}^{l} \bigvee_{r=0}^{n_k} (q_k^{r)}(y) > 0 \wedge \bigwedge_{u=1}^{r-1} q_k^{u)}(y) = 0),$$

Bj $c \neq 0 \land \bigvee y(q_j(y) = 0 \land \bigwedge_{k=1}^{l} (\bigwedge x(y < x \rightarrow q_k(x) \neq 0)) \land \bigwedge_{k=1}^{l} q_k(y+1) > 0),$

Cj $c \neq 0 \land \bigvee z(q_j(z) = 0 \land \bigwedge_{k=1}^{l} (\bigwedge x(x < z \rightarrow q_k(x) \neq 0)) \land \bigwedge_{k=1}^{l} q_k(z-1) > 0),$

D $c \neq 0 \land \bigwedge_{k=1}^{l} (\bigwedge x\; q_k(x) \neq 0) \land \bigwedge_{k=1}^{l} q_k(0) > 0).$

Finalmente obtenemos:

Teorema 2.40 (Tarski) *Toda fórmula de $\mathcal{L}_A$ es equivalente en* CRC *a una fórmula sin cuantificadores con las mismas variables libres.*

DEMOSTRACIÓN: Basta probar la hipótesis del teorema 2.34, pero la prueba es prácticamente idéntica a la del teorema 2.38, usando ahora el teorema anterior. ■

En particular, toda sentencia de $\mathcal{L}_A$ es equivalente en CRC a una sentencia sin cuantificadores, más concretamente a una disyunción de conjunciones de sentencias de tipo $m = 0$ o bien $m > 0$, donde m es un número entero. Como todas las sentencias de este tipo son demostrables o refutables en CRC, concluimos:

Teorema 2.41 CRC *es una teoría axiomática completa, es decir, toda sentencia puede demostrarse o refutarse a partir de sus axiomas.*

Combinando esto con la consistencia de la teoría, concluimos que CRC es una teoría *decidible:* existe un algoritmo que permite determinar en un número finito de pasos si una sentencia dada es o no un teorema de CRC. Para ello sólo hay que calcular una sentencia equivalente sin cuantificadores y demostrarla o refutarla (lo cual siempre es trivial).

Cuerpos algebraicamente cerrados Al igual que sucede con la prueba de consistencia, el teorema de eliminación de cuantificadores es válido también para la teoría CAC, con una demostración bastante más sencilla.

Observemos en primer lugar que el teorema 2.27 vale igualmente en este caso, y al particularizar a CAC el teorema 2.25 nos encontramos con que las fórmulas atómicas de $\mathcal{L}_A^-$ son todas de la forma $t_1 = t_2$, y son equivalentes a $t_1 - t_2 = 0$, luego se cumple 2.28 entendiendo por fórmulas elementales las de la forma

$$p_1 = 0 \land \cdots \land p_k = 0 \land q_1 \neq 0 \land \cdots \land q_l \neq 0.$$

Los teoremas 2.33 y 2.34 valen igualmente sin más que cambiar cada fórmula $q_j > 0$ por $q_j \neq 0$.

La prueba del teorema equivalente a 2.38 se reduce ahora a demostrar que toda fórmula de tipo

$$\bigvee x(c \neq 0 \land f = 0 \land q_1 \neq 0 \land \cdots \land q_l \neq 0),$$

donde c es un producto sin la variable x entre cuyos factores estén el coeficiente director de f y los de los q_j, es equivalente a una fórmula sin cuantificadores. Ahora bien, llamando $q = q_1 \cdots q_l$, es equivalente a

$$\bigvee x(c \neq 0 \land f = 0 \land q \neq 0).$$

Las condiciones $f = 0 \land q \neq 0$ equivalen a que el polinomio $f^d(X)$ asociado al término f tiene una raíz x que no es raíz del polinomio $q^m(X)$ asociado a q. Teniendo en cuenta que ambos se descomponen en factores irreducibles de grado 1 (porque todos los polinomios de grado no nulo tienen raíces) lo contrario equivale a que todos los factores irreducibles de $f^d(X)$ sean también factores irreducibles de $q^m(X)$. Como la máxima multiplicidad posible de una raíz de $f^d(X)$ es d, esto equivale a su vez a que $f^d(X) \mid q^m(X)^d$. Por lo tanto, la fórmula equivale a

$$c \neq 0 \land f^d(X) \nmid q^m(X)^d.$$

Aquí no aparece la variable x, pero esto no es una fórmula sin cuantificadores, pues éstos están implícitos en la definición de divisibilidad. Por el teorema 2.31 podemos expresar

$$c^{m-d+1}q^d = fq + r,$$

donde r tiene grado menor que d. Podemos escribirlo como $r = \sum_{i=0}^{d-1} a_i x^i$, donde los a_i son términos de $\mathcal{L}_A^-$ sin la variable x. Ahora bien, $f^d(X) \mid q^m(X)^d$ es equivalente a que $r^{d-1}(X) = 0$, o también a que $a_0 = \cdots = a_{d-1} = 0$. En definitiva, la fórmula dada es equivalente a

$$c \neq 0 \land (a_0 \neq 0 \lor \cdots \lor a_{d-1} \neq 0),$$

y ahora sí que tenemos una fórmula sin cuantificadores.

Finalmente, la prueba del resultado análogo a 2.40 se reduce a probar que toda fórmula de tipo

$$\bigvee x(c \neq 0 \land q_1 \neq 0 \land \cdots \land q_l \neq 0)$$

es equivalente a una fórmula sin cuantificadores, pero esto es trivial, pues si llamamos $q = q_1 \cdots q_l$, la fórmula equivale a

$$\bigvee x(c \neq 0 \land q \neq 0),$$

que a su vez es equivalente a $c \neq 0$, pues esto ya implica que el coeficiente director de q es distinto de 0, y por lo tanto q tiene un número finito de raíces. Como en CAC se cumple el esquema de infinitud, siempre existe un x que no sea raíz de q. Así pues:

Teorema 2.42 (Tarski) *Toda fórmula de $\mathcal{L}_A^-$ es equivalente en* CAC *a una fórmula sin cuantificadores con las mismas variables libres.*

En particular, toda sentencia es equivalente a una disyunción de conjunciones de fórmulas de tipo $m = 0$ o bien $m \neq 0$, donde m es un número entero. No obstante, estas fórmulas no son demostrables ni refutables en CAC, pero sí en las teorías CAC_p o CAC_0 que determinan la característica del cuerpo.

Concluimos que CAC_p y CAC_0 son teorías axiomáticas consistentes, completas y decidibles.

2.7 El esquema de completitud

El teorema de eliminación de cuantificadores nos permite probar en CRC algunos principios adicionales que, de hecho, es fácil ver que son equivalentes en CO a los distintos apartados del teorema 2.18:

Teorema 2.43 *Toda clase no vacía y acotada superiormente tiene supremo.*

Demostración: El enunciado es un esquema teoremático, con un caso particular para cada fórmula $\phi(x, x_1, \ldots, x_n)$ de $\mathcal{L}_A$, que afirma que si la clase $A = \{x \mid \phi(x)\}$ no es vacía y está acotada superiormente, entonces tiene supremo.

Por el teorema 2.40 tenemos que existen polinomios p_{ij}, q_{ij} tales que

$$\phi(x) \leftrightarrow \bigvee_{i=1}^{m} (p_{i1} = 0 \land \cdots \land p_{ik_i} = 0 \land q_{i1} > 0 \land \cdots \land q_{il_i} > 0).$$

Llamemos

$$A_i = \{x \mid p_{i1} = 0 \land \cdots \land p_{ik_i} = 0 \land q_{ij} > 0 \land \cdots \land q_{il_i} > 0\},$$

de modo que $A = \bigcup_{i=1}^{m} A_i$. Podemos suponer que todos los $A_i \neq \varnothing$, pues en caso contrario podríamos eliminar la fórmula i-ésima de la disyunción equivalente a ϕ. A su vez,

$$A_i = \bigcap_{j=1}^{k_i} \{x \mid p_{ij} = 0\} \cap \bigcap_{j=1}^{l_i} \{x \mid q_{ij} > 0\}.$$

Por 2.19 sabemos que $\{x \mid q_{ij} > 0\}$ es una unión finita de intervalos, y lo mismo vale trivialmente para $\{x \mid p_{ij} = 0\}$ (pues es $\varnothing$, $]-\infty, +\infty[$ o bien unión de intervalos degenerados $[a, a]$). Por la observación tras el teorema 2.1 lo mismo vale para cada A_i, luego también para A. Por 2.4 concluimos que A tiene supremo. ∎

Un caso particular, pero con una interpretación geométrica más simple, es el siguiente:

Teorema 2.44 *Sean A y B dos clases no vacías que satisfagan $R = A \cup B$ y $\bigwedge xy(x \in A \land y \in B \to x < y)$. Entonces $\bigvee s \bigwedge xy(x \in A \land y \in B \to x \leq s \leq y)$.*

Demostración: Los elementos de B son cotas superiores de A, luego basta tomar como s el supremo de A. ∎

Si C es una clase no vacía y acotada superiormente, entonces

$$A = \{x \mid \bigvee x'(x \leq c' \land x' \in C)\}, \qquad B = \{y \mid \bigwedge x(x \in C \to x < y)\}$$

están en las condiciones del teorema anterior y es fácil ver que el supremo de A es también el supremo de C, por lo que 2.43 puede probarse a partir del teorema anterior. Por ello, a cualquiera de los dos enunciados podemos llamarlo *esquema de completitud.*

Si añadimos como esquema axiomático a CO cualquiera de las dos versiones del esquema de completitud no es difícil demostrar la primera parte del teorema 2.18, por lo que el esquema de completitud es una forma equivalente de axiomatizar CRC.

La propiedad arquimediana El lector debería prestar atención al "teorema" siguiente, porque no es realmente demostrable en CRC y es fundamental comprender por qué el error de razonamiento en que incurrimos si lo aceptamos como válido no lo hemos cometido en ninguno de los resultados precedentes (ni en los que veremos más delante):

"Teorema" *Existe un número natural n tal que $|x| < n$.*

"Demostración": Sea A la clase de todos los x tales que existe un número natural n tal que $|x| < n$. Obviamente $0 \in A$, luego no es vacía. Tenemos que probar que $A = R$. En caso contrario, sea $c \notin A$. Cambiando c por $-c$ si es preciso, podemos suponer que $c > 0$. Entonces c es cota superior de A, ya que si $x \in A$, entonces existe un natural n tal que $x \leq |x| \leq n < y$, pues no puede ser $y \leq n$. Por el esquema de completitud A tiene un supremo s (claramente $s > 0$).

Si $s \in A$, entonces existe un n tal que $s < n$, pero entonces $s + 1 < n + 1$, luego $s + 1 \in A$, en contradicción con que s sea cota superior de A. Por lo tanto, tiene que ser $s \notin A$. Como $s - 1 < s$, no puede ser cota superior de A, luego existe un $x \in A$ tal que $s - 1 \leq x < s$, pero entonces existe un n tal que $s - 1 < n$, luego $s < n + 1$, y de nuevo tenemos una contradicción. ■

El error está en que el enunciado del "teorema" no puede interpretarse ni como una fórmula de $\mathcal{L}_A$ ni como un esquema teoremático. La *propiedad arquimediana* que pretende formalizar el enunciado no es, de hecho, formalizable en CRC.

En muchas ocasiones hemos formulado enunciados que postulaban la existencia de números naturales como disyunciones de fórmulas cada una de las cuales dependía de un número natural en particular, pero en este caso necesitaríamos una disyunción infinita:

$$|x| < 1 \lor |x| < 2 \lor |x| < 3 \lor \cdots$$

que no tiene sentido. Y un esquema teoremático puede hacer las veces de conjunción infinita, pero no de disyunción infinita. En particular, la clase A de la demostración no está bien definida.

Tal vez el lector pueda objetar que, aunque ciertamente el enunciado y la prueba no son correctos, podría haber otra forma distinta de enunciar y demostrar la propiedad arquimediana en CRC, pero podemos demostrar que no es así. Para ello basta añadir a $\mathcal{L}_A$ una nueva constante c y añadir a CRC como axiomas las sentencias

$$c > 0, \quad c > 1, \quad c > 2, \quad c > 3, \quad \ldots$$

La teoría resultante es consistente, pues si pudiera demostrarse una contradicción a partir de ella, la prueba emplearía sólo un número finito de los axiomas adicionales, pero la adición de un número finito de estos axiomas es consistente, ya que tiene por modelo a cualquier modelo de CRC en el que la constante c se interpreta como un número natural suficientemente grande.

Por lo tanto, un modelo de esta extensión de CRC es un modelo de CRC en el que existe un número mayor que todos los números naturales, luego no es posible demostrar lo contrario en CRC.

2.8 Teoría de modelos

Los resultados sobre eliminación de cuantificadores en CRC y CAC pueden demostrarse de una forma mucho más rápida, aunque no constructiva, en el contexto de la teoría de modelos formalizada en la teoría de conjuntos. En esta sección describiremos este enfoque.

Observemos que la consistencia de CRC y CAC es trivial en este contexto, pues CRC admite un modelo. De hecho, los modelos de CRC son exactamente los cuerpos realmente cerrados,[11] como $\mathbb{R}$ o el conjunto R de los números reales algebraicos, mientras que los modelos de CAC son los cuerpos algebraicamente cerrados. Más concretamente, $\mathbb{C}$ o la clausura algebraica de $\mathbb{Q}$ son modelos de CAC_0 y la clausura algebraica del cuerpo de p elementos es un modelo de CAC_p.

Definición 2.45 Diremos que una teoría axiomática T sobre un lenguaje de primer orden $\mathcal{L}$ *admite eliminación de cuantificadores* si para cada fórmula $\phi(x_1, \ldots, x_n)$ de $\mathcal{L}$ existe otra fórmula $\psi(x_1, \ldots, x_n)$ sin cuantificadores y con las mismas variables libres tal que $\vdash_T (\phi \leftrightarrow \psi)$.

Por el teorema de completitud, la condición $\vdash_T (\phi \leftrightarrow \psi)$ es equivalente a $\vDash_T (\alpha \leftrightarrow \beta)$, es decir, a que $\phi \leftrightarrow \psi$ sea verdadera en todos los modelos de T.

Teorema 2.46 *Sea T una teoría axiomática sobre un lenguaje $\mathcal{L}$ que posea al menos una constante y sea $\phi(x_1, \ldots, x_n)$ una fórmula de $\mathcal{L}$. Entonces existe una fórmula ψ sin cuantificadores y con las mismas variables libres tal que $\vDash_T (\phi \leftrightarrow \psi)$ si y sólo si cuando M y N son modelos de T y C es un submodelo común a ambos, se cumple*

$$\bigwedge a_1, \ldots, a_n \in C (M \vDash \phi[a_1, \ldots, a_n] \leftrightarrow N \vDash \phi[a_1, \ldots, a_n]).$$

[11] Véase el teorema 7.65 de [Al].

Demostración: Si existe la fórmula ψ y $a_1,\ldots,a_n\in C$, entonces

$$M\vDash\phi[a_1,\ldots,a_n]\leftrightarrow M\vDash\psi[a_1,\ldots,a_n]\leftrightarrow C\vDash\psi[a_1,\ldots,a_n]$$

$$\leftrightarrow N\vDash\psi[a_1,\ldots,a_n]\leftrightarrow N\vDash\phi[a_1,\ldots,a_n],$$

donde hemos usado que, obviamente, las fórmulas sin cuantificadores se cumplen en un modelo si y sólo si se cumplen en un submodelo.

Supongamos ahora que se cumple la condición del enunciado. Si $T\vdash\phi$, basta tomar $\psi\equiv x_1=x_1\land\cdots\land x_n=x_n$ (o $c=c$ si ϕ no tiene variables libres, donde c es una constante de $\mathcal{L}$). Si $T\vdash\neg\phi$, tomamos $\psi\equiv x_1\neq x_1\land\cdots\land x_n\neq x_n$ (o $c\neq c$).

Así pues, podemos suponer que ni ϕ ni $\neg\phi$ son teoremas de T. Llamamos Γ al conjunto de todas las fórmulas $\psi(x_1,\ldots,x_n)$ cuyas variables libres estén entre las indicadas tales que $\vdash_T(\phi\rightarrow\psi)$.

Añadamos a $\mathcal{L}$ nuevas constantes $d_1,\ldots,d_n$ y sea $\Gamma(d_1,\ldots,d_n)$ el conjunto de sentencias que resultan de sustituir las variables $x_1,\ldots,x_n$ de cada fórmula de Γ por $d_1,\ldots,d_n$.

Veamos que si añadimos $\Gamma(d_1,\ldots,d_n)$ a los axiomas de T podemos demostrar $\phi(d_1,\ldots,d_n)$.

En caso contrario, existe un modelo M de T, $\Gamma(d_1,\ldots,d_n)$ y $\neg\phi(d_1,\ldots,d_n)$.

Sean $\bar{d}_1,\ldots,\bar{d}_n\in M$ los objetos denotados por las constantes, y sea C el submodelo mínimo de M, es decir, $C=\{M(t)\mid t\text{ es un designador de }\mathcal{L}^*\}$, donde $\mathcal{L}^*$ indica el lenguaje que resulta de haber añadido a $\mathcal{L}$ las nuevas constantes. Notemos que como $\mathcal{L}$ contiene al menos una constante, $C\neq\varnothing$.

Llamemos $D(C)$ el conjunto de las sentencias atómicas y negaciones de sentencias atómicas de $\mathcal{L}^*$ que son verdaderas en C y sea Σ el conjunto formado por los axiomas de T, $D(C)$ y $\phi(d_1,\ldots,d_n)$.

Vamos a probar que Σ es consistente. En caso contrario a partir de T y $D(C)$ puede probarse $\neg\phi(d_1,\ldots,d_n)$ y, más concretamente, existen sentencias $\psi_1,\ldots,\psi_m\in D(C)$ tales que

$$\vdash_T(\psi_1\land\cdots\land\psi_m\rightarrow\neg\phi(d_1,\ldots,d_n)).$$

Cada sentencia ψ_i puede verse como $\psi_i'(d_1,\ldots,d_n)$, para cierta fórmula atómica $\psi'(x_1,\ldots,x_n)$, y que la implicación anterior sea verdadera en todo modelo de $\mathcal{L}^*$ equivale a que

$$\vDash_T\bigwedge x_1\cdots x_n(\psi_1'\land\cdots\land\psi_m'\rightarrow\neg\phi),$$

pero entonces $\vdash_T(\phi\vdash\neg\psi_1'\lor\cdots\lor\neg\psi_m')$, luego $\neg\psi_1'\lor\cdots\lor\neg\psi_m'\in\Gamma$, luego $\neg\psi_1\lor\cdots\lor\neg\psi_m\in\Gamma(d_1,\ldots,d_n)$, luego $M\vDash\neg\psi_1\lor\cdots\lor\neg\psi_m$, luego también $C\vDash\neg\psi_1\lor\cdots\lor\neg\psi_m$, en contradicción con que $\psi_i\in D(C)$ para todo i.

Sea, pues N un modelo de Σ. Como $D(C)\subset\Sigma$, es claro que $M(t)\mapsto N(t)$ define un isomorfismo de C en el modelo mínimo de N. (Notemos, por ejemplo,

que si $M(t) = M(t')$, entonces $t = t' \in D(C) \subset \Sigma$, luego $N(t) = N(t')$, luego la aplicación está bien definida.)

Podemos suponer entonces que $C \subset N$ y entonces por hipótesis

$$M \vDash \phi[\bar{d}_1, \ldots, \bar{d}_n] \leftrightarrow N \vDash \phi[\bar{d}_1, \ldots, \bar{d}_n],$$

es decir,

$$M \vDash \phi(d_1, \ldots, d_n) \leftrightarrow N \vDash \phi(d_1, \ldots, d_n),$$

con lo que tenemos una contradicción.

Con esto tenemos probado que $\Gamma(d_1, \ldots, d_n) \vdash_T \phi(d_1, \ldots, d_n)$, luego existen $\psi_1, \ldots, \psi_m \in \Gamma$ tales que

$$\vDash_T (\psi_1(d_1, \ldots, d_n) \wedge \cdots \wedge \psi_m(d_1, \ldots, d_n) \rightarrow \phi(d_1, \ldots, d_n),$$

pero esto es lo mismo que

$$\vDash_T (\psi_1 \wedge \cdots \wedge \psi_m \rightarrow \phi),$$

y la otra implicación se cumple por definición de Γ, luego

$$\vdash_T (\phi \leftrightarrow \psi_1 \wedge \cdots \wedge \psi_m)$$

y así la fórmula $\psi \equiv \psi_1 \wedge \cdots \wedge \psi_m$ cumple lo requerido. ■

Tenemos así una caracterización de la eliminación de cuantificadores en términos de la teoría de modelos. Veamos cómo se aplica:

Teorema 2.47 *La teoría* CRC *admite eliminación de cuantificadores.*

Demostración: Por la observación tras el teorema 2.28, basta probar que las fórmulas de tipo

$$\bigvee x\, (p_1 = 0 \wedge \cdots \wedge p_k = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0),$$

donde p_i, q_1 son polinomios en x cuyos coeficientes tienen libres las variables $x_1, \ldots, x_n$, son equivalentes a fórmulas sin cuantificadores. Para ello aplicamos el criterio que proporciona el teorema anterior.

Suponemos que M y N son dos modelos de CRC con un submodelo en común C y suponemos que existen $a_1, \ldots, a_n \in C$ tales que existe un $a \in M$ tal que

$$M \vDash (p_1 = 0 \wedge \cdots \wedge p_k = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0)[a, a_1, \ldots, a_n],$$

y tenemos que probar que existe un $a' \in N$ que cumple lo mismo.

Notemos que C no es necesariamente un modelo de CRC, pero por ser un submodelo de M tenemos claramente que es un dominio íntegro.[12] No obstante, podemos considerar, tanto en M como en N la clausura real del cuerpo de cocientes K de C (que no es sino el cuerpo formado por los elementos de M o

[12]no podemos asegurar que sea un cuerpo porque $\mathcal{L}_A$ no incluye un funtor $(\ )^{-1}$, luego la existencia de inverso en M no asegura que exista en C.

N algebraicos sobre K). La unicidad de la clausura real[13] implica que ambas son K-isomorfas, por lo que podemos identificarlas con un mismo subcuerpo realmente cerrado $R \subset M \cap N$.

Si alguno de los polinomios p_i no es idénticamente nulo (al interpretar sus coeficientes con $a_1, \ldots, a_n$), entonces a es algebraico sobre K, luego $a \in R \subset N$. En caso contrario, cualquier $a' \in N$ cumple trivialmente

$$N \vDash (p_1 = 0 \wedge \cdots \wedge p_k = 0)[a', a_1, \ldots, a_n],$$

y se trata de encontrar un $a' \in N$ que cumpla la parte correspondiente a los q_i.

Ahora bien, cada q_i (con sus coeficientes interpretados con $a_1, \ldots, a_n$) se descompone en $R[X]$ como producto de factores primos de grado 1 o 2. Los de grado 2 tienen signo constante, mientras que los de grado 1 cambian de signo sólo una vez. Por lo tanto, podemos encontrar un número finito de intervalos $]\alpha_i, \beta_i[$ con extremos en R o bien $\pm\infty$, de modo que

$$M \vDash (q_1 > 0 \wedge \cdots \wedge q_l > 0)[a, a_1, \ldots, a_n] \leftrightarrow a \in \bigcup_i]\alpha_i, \beta_i[\,,$$

luego podemos tomar un a' que esté en $R \subset N$ y en dicha unión, y así a' cumple lo requerido. ■

Simplificando la prueba anterior obtenemos:

Teorema 2.48 *La teoría* CAC *admite eliminación de cuantificadores.*

Una consecuencia inmediata de la eliminación de cuantificadores es la siguiente:

Teorema 2.49 *Si una teoría T admite eliminación de cuantificadores y $M \subset N$ son dos modelos de T, se cumple que $M \prec N$.*

Por otra parte, a partir de aquí se prueba también sin dificultad el teorema 2.41 que nos da que CRC es completa, luego en particular todos sus modelos son elementalmente equivalentes, y en particular todos son elementalmente equivalentes a $\mathbb{R}$. Así pues, en CRC se puede demostrar cualquier propiedad de $\mathbb{R}$ expresable en el lenguaje $\mathcal{L}_A$.

Lo mismo es válido para CAC_0 con $\mathbb{C}$ en lugar de $\mathbb{R}$, y para las teorías CAC_p con la clausura algebraica del cuerpo de p-elementos.

Nota Hemos visto que una axiomatización alternativa de CRC consiste en eliminar el relator > 0 y tomar como axiomas los de C más **CRC1**, **CRC2**, **CRC3** (véase la página 57) tomando **CRC4** como una definición. Terminamos con la observación de que esta teoría no admite eliminación de cuantificadores. Por ejemplo, la fórmula

$$x > 0 \equiv x \neq 0 \wedge \bigvee u(x = u^2)$$

no es equivalente a ninguna fórmula sin cuantificadores (en la axiomatización inicial de CRC es ella misma una fórmula sin cuantificadores).

[13]Teorema 8.58 de [AL].

Para probarlo consideramos el cuerpo ordenado $C = \mathbb{Q}[\sqrt{2}]$ con el orden usual (heredado de $\mathbb{R}$) al que llamaremos $\leq_1$. Puesto que la conjugación dada por $\alpha = a + b\sqrt{2} \mapsto \bar{\alpha} = a - b\sqrt{2}$ es un automorfismo de cuerpos, resulta que $\mathbb{Q}[\sqrt{2}]$ también es un cuerpo ordenado con la relación $\alpha \leq_2 \beta \leftrightarrow \bar{\alpha} \leq_1 \bar{\beta}$.

Llamamos $\alpha = \sqrt{2}$, de modo que $\alpha >_1 0$ y $\alpha <_2 0$. Sean M y N clausuras reales de $(C, \leq_1)$ y $(C, \leq_2)$, respectivamente. Ambas son modelos de CRC, pero, al considerarlas como teorías sobre $\mathcal{L}_A^-$, tenemos que C (sin especificar en él una relación de orden) es un submodelo de ambas (no lo sería si consideráramos el relator > 0), pero $M \vDash [\alpha] > 0$ y $N \vDash \neg[\alpha] > 0$, y basta aplicar el teorema 2.46.

■

2.9 El decimoséptimo problema de Hilbert

Una aplicación notable de los resultados anteriores es la solución al problema decimoséptimo de Hilbert. Hilbert había conjeturado que todo polinomio de $\mathbb{R}[x_1, \ldots, x_n]$ que no tomara valores negativos debía de poder expresarse como suma de cuadrados de otros polinomios. Sin embargo, Minkowski lo convenció de que eso era probablemente falso y finalmente Hilbert lo demostró en 1888, aunque con una prueba no constructiva que no daba un contraejemplo explícito. El primer contraejemplo explícito lo dio T. Motzkin en 1997:

$$M(x, y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2.$$

La desigualdad entre la media aritmética y la geométrica nos da que

$$\frac{x^4y^2 + x^2y^4 + 1}{3} \geq \sqrt[3]{x^6y^6} = x^2y^2,$$

de donde $M(x, y) \geq 0$ para todo $(x, y) \in \mathbb{R}^2$. Sin embargo, supongamos que

$$M = \sum_{i=1}^{n} f_i(x, y)^2,$$

para ciertos polinomios $f_i \in \mathbb{R}[x, y]$ (necesariamente de grado ≤ 3).

Como $M(x, 0) = M(0, y) = 1$, los polinomios $f_i(x, 0)$ y $f_i(0, y)$ tienen que ser constantes, pues la suma de los dobles de sus grados es igual a 0. Por lo tanto, cada f_i es de la forma

$$f_i = a_i + b_ixy + c_ix^2y + d_ixy^2,$$

pero entonces el coeficiente -3 que aparece en M junto al término x^2y^2 debería ser

$$-3 = b_1^2 + \cdots + b_n^2,$$

lo cual es imposible.

En 1 893, Hilbert demostró, con un razonamiento muy complicado, que todo polinomio de $\mathbb{R}[x, y]$ que no toma valores negativos puede expresarse como suma

de cuadrados de funciones racionales en $\mathbb{R}(x, y)$. Por ejemplo,

$$M(x,y) = \frac{(x^2+y^2+1)x^2y^2(x^2+y^2-2)^2+(x^2-y^2)^2}{(x^2+y^2)^2},$$

de donde, sin más que desarrollar el primer producto del numerador, se desprende una descomposición en suma de cuatro cuadrados de funciones racionales.

En 1900, Hilbert incluyó en la lista de problemas que presentó en el Congreso Internacional de Matemáticos de París la pregunta de si todo polinomio de $\mathbb{R}[x_1, \ldots, x_n]$ que no tome valores negativos se puede expresar como suma de cuadrados de funciones racionales de $\mathbb{R}(x_1, \ldots, x_n)$.

En 1927 Artin dio una prueba no constructiva de la conjetura de Hilbert y en 1940 Habicht dio una prueba constructiva.

Aquí vamos a dar una prueba no constructiva debida a Robinson:

Teorema 2.50 *Todo polinomio de $\mathbb{R}[x_1, \ldots, x_n]$ que no tome valores negativos se expresa como suma de cuadrados en el cuerpo de cocientes $R(x_1, \ldots, x_n)$.*

DEMOSTRACIÓN: Supongamos que $f(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$ no es una suma de cuadrados en $R(x_1, \ldots, x_n)$. Entonces[14] existe una relación de orden compatible con la estructura algebraica respecto de la cual f es negativo. Sea R la clausura real de $R(x_1, \ldots, x_n)$ respecto de dicho orden. Entonces las indeterminadas $x_1, \ldots, x_n \in R$ cumplen $f(x_1, \ldots, x_n) < 0$, es decir,

$$R \vDash \bigvee u_1 \cdots u_n \; f(u_1, \ldots, u_n) < 0,$$

pero esta sentencia tiene que ser verdadera en cualquier cuerpo realmente cerrado, en particular en $\mathbb{R}$, luego

$$\mathbb{R} \vDash \bigvee u_1 \cdots u_n \; f(u_1, \ldots, u_n) < 0,$$

y esto significa que f toma valores negativos. ■

[14]Teorema 7.62 de [Al]. Notemos que $R(x_1, \ldots, x_n)$ es un cuerpo real porque -1 no es suma de cuadrados (teorema 7.59).

Segunda parte

La geometría elemental

Capítulo III

Los elementos de la geometría de Tarski

El lenguaje formal de la geometría de Tarski es bastante austero, pues consta únicamente de tres conceptos no definidos (además de las variables y signos lógicos, incluyendo el igualador):

Punto No tiene asociado ningún signo en el lenguaje formal, porque simplemente llamaremos "puntos" a los objetos a los que hacen referencia las variables. La interpretación pretendida es el concepto intuitivo de "punto" como posición inextensa en el espacio que todos conocemos.

Ordenación El relator de ordenación es un relator triádico que representaremos por $a - b - c$ y que leeremos "el punto b está entre los puntos a y c". Su interpretación pretendida es que los puntos a, b, c están alineados y b está entre los otros dos, con el convenio de que entre los puntos situados entre a y c se encuentran los propios a y c, de modo que las afirmaciones $a - a - c$ y $a - c - c$ serán siempre verdaderas.

Congruencia Se trata de un relator tetrádico que representaremos por $\overline{ab} \equiv \overline{cd}$ y que leeremos "el segmento $\overline{ab}$ es congruente con el segmento $\overline{cd}$". Se interpreta como que la distancia del punto a al punto b es la misma que la distancia del punto c al punto d.

Naturalmente los significados pretendidos se dan sólo a título orientativo. Técnicamente hay que entender que simplemente hemos definido un lenguaje formal de primer orden cuyos únicos signos eventuales son un relator triádico y un relator tetrádico.

3.1 Los axiomas básicos

Presentamos seguidamente los ocho primeros axiomas de la geometría de Tarski.

Los axiomas básicos de la geometría de Tarski:

A1	$\overline{ab} \equiv \overline{ba}$
A2	$\overline{ab} \equiv \overline{pq} \land \overline{ab} \equiv \overline{rs} \to \overline{pq} \equiv \overline{rs}$
A3	$\overline{ab} \equiv \overline{cc} \to a = b$
A4	$\bigvee x(q - a - x \land \overline{ax} \equiv \overline{bc})$
A5	$a \neq b \land a - b - c \land a' - b' - c'$ $\land \overline{ab} \equiv \overline{a'b'} \land \overline{bc} \equiv \overline{b'c'} \land \overline{ad} \equiv \overline{a'd'} \land \overline{bd} \equiv \overline{b'd'} \to \overline{cd} \equiv \overline{c'd'}$
A6	$a - b - a \to a = b$
A7	$a - p - b \land q - c - b \to \bigvee x(p - x - q \land c - x - a)$
A8	$\bigvee abc(\neg a - b - c \land \neg b - c - a \land \neg c - a - b)$

Los dos primeros axiomas afirman esencialmente que la congruencia es una relación de equivalencia. Concretamente:

Teorema 3.1 *Se cumple:*

1. $\overline{ab} \equiv \overline{ab}$,
2. $\overline{ab} \equiv \overline{pq} \to \overline{pq} \equiv \overline{ab}$,
3. $\overline{pq} \equiv \overline{ab} \land \overline{ab} \equiv \overline{rs} \to \overline{pq} \equiv \overline{rs}$.

DEMOSTRACIÓN: Para la propiedad reflexiva aplicamos **A2** como sigue:

$$\overline{ab} \equiv \overline{pq} \land \overline{ab} \equiv \overline{rs} \to \overline{pq} \equiv \overline{rs}$$
$$\overline{ba} \equiv \overline{ab} \land \overline{ba} \equiv \overline{ab} \to \overline{ab} \equiv \overline{ab}$$

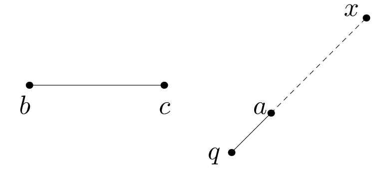
(La primera línea es el axioma **A2** tal cual lo hemos enunciado, y la segunda es el caso particular que necesitamos aquí.) La hipótesis de la implicación se cumple por **A1**.

Para la propiedad simétrica aplicamos así el axioma **A2**:

$$\overline{ab} \equiv \overline{pq} \land \overline{ab} \equiv \overline{rs} \to \overline{pq} \equiv \overline{rs}$$
$$\overline{ab} \equiv \overline{pq} \land \overline{ab} \equiv \overline{ab} \to \overline{pq} \equiv \overline{ab}$$

Como $\overline{ab} \equiv \overline{ab}$ se cumple por la parte ya probada, la conclusión es inmediata. La transitividad ya está expresada en el axioma **A2**, pero la simetría permite expresarla ahora en la forma alternativa dada en el enunciado. ■

El axioma **A3** afirma simplemente que todo segmento congruente a otro de extremos iguales tiene necesariamente extremos iguales. El axioma **A4** afirma que a partir de todo segmento $\overline{bc}$ se puede construir otro segmento congruente que prolongue al segmento $\overline{qa}$:



El axioma **A4**.

Con este axioma podemos demostrar que todo par de segmentos con extremos iguales son congruentes:

Teorema 3.2 $\overline{aa} \equiv \overline{bb}$.

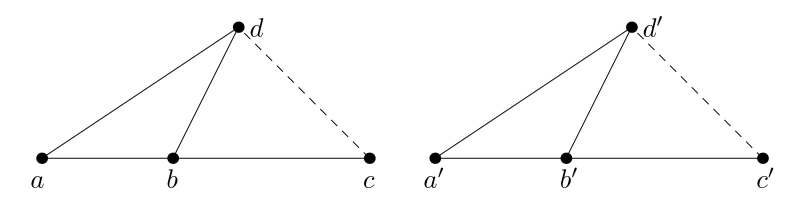
DEMOSTRACIÓN: Aplicamos como sigue el axioma **A4**:

$$\bigvee x(q - a - x \land \overline{ax} \equiv \overline{bc})$$

$$\bigvee x(b - a - x \land \overline{ax} \equiv \overline{bb})$$

Así pues, existe un punto x tal que $b - a - x$ y $\overline{ax} \equiv \overline{bb}$. Por el axioma **A3** tiene que ser $a = x$, luego $\overline{aa} \equiv \overline{bb}$. ■

El axioma **A5** es conocido como el *axioma de los cinco segmentos:*



Axioma de los cinco segmentos

Afirma que si tenemos dos figuras como las indicadas en las que los cuatro segmentos mostrados de una de ellas son congruentes con los cuatro correspondientes en la otra, entonces también lo son los segmentos trazados con línea discontinua.

La idea es que los triángulos $\widehat{abc}$ y $\widehat{a'b'c'}$ tienen sus lados iguales, luego también sus ángulos, por lo que los triángulos $\widehat{acd}$ y $\widehat{a'c'd'}$ tienen iguales dos lados y el ángulo que forman, luego también el tercer lado. No obstante, hay que tener presente que la figura sólo muestra un caso particular del axioma, ya que éste no exige, por ejemplo, que los cuatro puntos no sean colineales, ni que sean distintos dos a dos. El lector puede comprobar que todos los casos posibles del axioma son intuitivamente verdaderos.

Conviene introducir la notación

$$\mathrm{Ext}\begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} \leftrightarrow$$

$$a - b - c \land a' - b' - c' \land \overline{ab} \equiv \overline{a'b'} \land \overline{bc} \equiv \overline{b'c'} \land \overline{ad} \equiv \overline{a'd'} \land \overline{bd} \equiv \overline{b'd'}$$

(y diremos que los ocho puntos forman una *configuración exterior de cinco segmentos*), de modo que el axioma **A5** afirma que

$$a \neq b \land \mathrm{Ext}\begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} \to \overline{cd} \equiv \overline{c'd'}.$$

El teorema siguiente afirma esencialmente que es posible definir una suma de segmentos:

Teorema 3.3 $a - b - c \wedge a' - b' - c' \wedge \overline{ab} \equiv \overline{a'b'} \wedge \overline{bc} \equiv \overline{b'c'} \to \overline{ac} \equiv \overline{a'c'}$.

DEMOSTRACIÓN: Distinguimos dos casos: Si $a \neq b$, entonces podemos aplicar **A5**, porque se cumple Ext $\begin{pmatrix} a & b & c & a \\ a' & b' & c' & a' \end{pmatrix}$ (aquí usamos el teorema 3.2 y el axioma **A1**). La conclusión es que $\overline{ac} \equiv \overline{a'c'}$, como había que probar.

Si $a = b$ no podemos aplicar **A5**, pero se cumple que $\overline{aa} \equiv \overline{a'b'}$, luego $a' = b'$ por **A3**, y entonces la congruencia $\overline{bc} \equiv \overline{b'c'}$ que tenemos por hipótesis equivale a $\overline{ac} \equiv \overline{a'c'}$, que es lo que queremos concluir. ■

Otra aplicación elemental de **A5** es la unicidad del axioma **A4**:

Teorema 3.4 $q \neq a \to \overset{1}{\bigvee} x(q - a - x \wedge \overline{ax} \equiv \overline{bc})$.

DEMOSTRACIÓN: La existencia de x la da el axioma **A4**. Sólo tenemos que probar la unicidad. Para ello suponemos que tenemos otro punto x' que cumple lo mismo, es decir, que

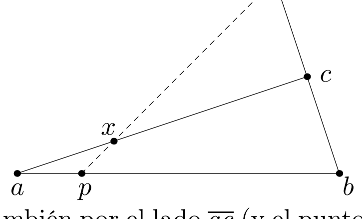
$$q - a - x \wedge \overline{ax} \equiv \overline{bc} \wedge q - a - x' \wedge \overline{ax'} \equiv \overline{bc}.$$

El teorema anterior nos da entonces que $\overline{qx} \equiv \overline{qx'}$ y la transitividad de la congruencia que $\overline{ax} \equiv \overline{ax'}$. Esto a su vez nos da la configuración

$$\operatorname{Ext}\begin{pmatrix} q & a & x & x \\ q & a & x & x' \end{pmatrix}.$$

Como además tenemos por hipótesis que $q \neq a$, podemos aplicar **A5** para concluir que $\overline{xx} \equiv \overline{xx'}$, luego por **A3** concluimos que $x = x'$. ■

La interpretación del axioma **A6** es inmediata, mientras que **A7** expresa un hecho nada trivial que Euclides asumió tácitamente. Se conoce como *axioma de Pasch:*



Tenemos un triángulo $\widehat{abc}$ y una recta pq que pasa por el lado $\overline{ab}$, pero no por el lado $\overline{bc}$ (pues pasa por el punto q, que está fuera de dicho lado). Entonces la recta tiene que pasar también por el lado $\overline{ac}$ (y el punto de corte está en el segmento $\overline{pq}$).

Nuevamente hay que tener presente que este axioma incluye los casos degenerados en los que, por ejemplo, los puntos son colineales, o algunos de ellos coinciden, etc. También es importante no confundir este axioma con el teorema 3.72, cuyo enunciado es muy similar, pero que no estaremos en condiciones de probar hasta mucho más adelante.

Por último, el axioma **A8** afirma la existencia de tres puntos no colineales.

3.2 Primeras consecuencias de los axiomas

Los axiomas que hemos dado contienen“condensada” de forma artificial una buena parte de la geometría euclídea, y “desempaquetar” toda la información que contienen es un proceso no menos artificial, que exige razonamientos sofisticados para probar hechos intuitivamente evidentes, mucho más evidentes que los axiomas a partir de los cuales los demostramos.

Para entender correctamente el sentido de este proceso hay que tener presente que su objetivo no es convencer al lector de unos resultados geométricos de por sí evidentes, sino demostrar algo que no es evidente en absoluto, y es que todos ellos son consecuencias lógicas de los pocos axiomas que hemos dado. Una vez hayamos “descomprimido” la geometría a partir del paquete axiomático dado, podremos razonar con la misma naturalidad que en cualquier otro texto de geometría, sabiendo que los hechos elementales en los que se basa cada paso de un razonamiento son todos demostrables a partir de los axiomas.

3.2.1 Más propiedades de ordenación

En la sección anterior hemos obtenido ya algunas primeras consecuencias de los axiomas, pero éstas hacían referencia principalmente a la relación de congruencia. Ahora vamos a probar algunos hechos elementales sobre la relación de ordenación.

Teorema 3.5 *Se cumple:*

1. $a-b-b \wedge a-a-b$,
2. $a-b-c \rightarrow c-b-a$,
3. $a-b-c \wedge b-a-c \rightarrow a=b$.

DEMOSTRACIÓN: 1) Por **A4** existe un punto x tal que $a-b-x \wedge \overline{bx} \equiv \overline{bb}$, por **A3** es $b=x$, luego $a-b-b$.

Veamos ahora 2), que a su vez implica trivialmente la segunda parte de 1).

Usamos el axioma **A7** (como es habitual lo copiamos tal y como lo hemos enunciado y debajo escribimos el caso particular que vamos a usar):

$$a-p-b \wedge q-c-b \rightarrow \bigvee x(p-x-q \wedge c-x-a)$$
$$a-b-c \wedge b-c-c \rightarrow \bigvee x(b-x-b \wedge c-x-a)$$

Las hipótesis de la implicación se cumplen por la hipótesis de 2) y por la parte ya probada de 1), luego existe un punto x en las condiciones indicadas, que por **A6** no es sino $x=b$, luego $c-b-a$.

3) Usamos de nuevo **A7**:

$$a-p-b \wedge q-c-b \rightarrow \bigvee x(p-x-q \wedge c-x-a)$$
$$a-b-c \wedge b-a-c \rightarrow \bigvee x(b-x-b \wedge a-x-a)$$

Por **A6** concluimos que $a=x=b$. ■

La tercera parte del teorema anterior, combinada con las dos anteriores, afirma que en la relación $a - b - c$ los extremos son intercambiables, pero los términos medios no lo son, es decir, que no puede suceder que tres puntos satisfagan dos relaciones de tipo $a-b-c$ con dos puntos distintos como término medio.

El relator de ordenación recibe este nombre porque sus propiedades contienen esencialmente la idea de que los puntos de una recta se pueden ordenar (de dos formas: "de izquierda a derecha" o "de derecha a izquierda"). Todavía no estamos en condiciones de demostrar esto, pero el teorema siguiente, que usaremos con frecuencia, contiene algunas consecuencias de este hecho general. El lector debería dibujarse puntos sobre una recta en las hipótesis de cada apartado hasta convencerse de que los enunciados expresan hechos intuitivamente claros:

Teorema 3.6 *Se cumple:*

1. $p - a - c \land a - b - c \to p - a - b \land p - b - c$,
2. $a - b - c \land a - c - p \to b - c - p \land a - b - p$,
3. $a - b - c \land b - c - d \land b \neq c \to a - c - d \land a - b - d$.

DEMOSTRACIÓN: Veamos la primera parte de 1). Para ello usamos **A7**:

$$a - p - b \land q - c - b \to \bigvee x(p - x - q \land c - x - a)$$

$$p - a - c \land a - b - c \to \bigvee x(a - x - a \land b - x - p)$$

Por **A6** tenemos que $x = a$, luego $b - a - p$, que equivale a $p - a - b$.

Ahora usamos esto para probar la primera parte de 2):

$$p - a - c \land a - b - c \to p - a - b$$

$$p - c - a \land c - b - a \to p - c - b$$

Como el relator de ordenación permite intercambiar los extremos, tenemos claramente la primera parte de 2). Ahora probamos la primera parte de 3). Empezamos usando **A4**:

$$\bigvee x(q - a - x \land \overline{ax} \equiv \overline{bc})$$

$$\bigvee x(a - c - x \land \overline{cx} \equiv \overline{cd})$$

Ahora usamos la parte ya probada de 2):

$$a - b - c \land a - c - p \to b - c - p$$

$$a - b - c \land a - c - x \to b - c - x$$

Tenemos $b - c - x$ y $b - c - d$, con $\overline{cx} \equiv \overline{cd}$. Como $b \neq c$, el teorema 3.4 implica que $x = d$, luego $a - c - d$.

Ahora probamos la segunda parte de 1). Observemos que si $a = b$ hay que probar $p - a - c$, que es una de las hipótesis, luego podemos suponer que $a \neq b$ y aplicamos la parte ya probada de 3):

$$a - b - c \wedge b - c - d \wedge b \neq c \rightarrow a - c - d$$

$$p - a - b \wedge a - b - c \wedge a \neq b \rightarrow p - b - c$$

Observemos que $p - a - b$ lo tenemos por la parte ya probada de 1), luego tenemos la conclusión $p - b - c$.

Ahora usamos esto para probar la segunda parte de 2):

$$p - a - c \wedge a - b - c \rightarrow p - b - c$$

$$p - c - a \wedge c - b - a \rightarrow p - b - a$$

El antecedente es equivalente a las hipótesis de 2), luego tenemos $p - b - a$, que equivale a su vez a $a - b - p$.

Por último probamos la segunda parte de 3) usando la parte ya probada:

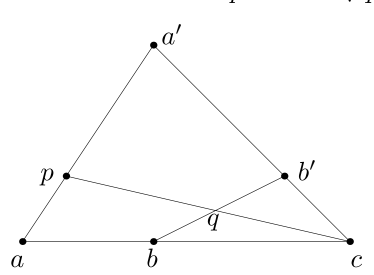
$$a - b - c \wedge b - c - d \wedge b \neq c \rightarrow a - c - d$$

$$d - c - b \wedge c - b - a \wedge c \neq b \rightarrow d - b - a$$

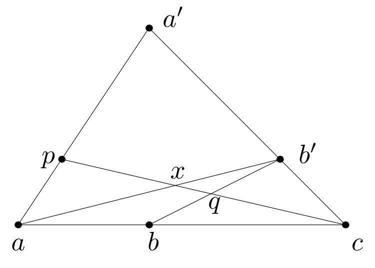
Así obtenemos $d - b - a$ y, por consiguiente, $a - b - c$. ■

He aquí otro resultado técnico que vamos a necesitar:

Teorema 3.7 $a - b - c \wedge a' - b' - c \wedge a - p - a' \rightarrow \bigvee q(p - q - c \wedge b - q - b')$.



Demostración: Vamos a aplicar dos veces **A7**. La primera al triángulo $\widehat{ab'a'}$. Por **A7** la recta cp tiene que cortar al lado $\overline{ab'}$ en un punto x que cumple $p - x - c \wedge a - x - b'$.



Ahora aplicamos **A7** al triángulo $\widehat{abb'}$. La recta cx tiene que cortar al lado $\overline{bb'}$ en un punto q que cumple $c - x - q \wedge b - q - b'$. Finalmente usamos el teorema 3.6, 1):

$$p - a - c \wedge a - b - c \rightarrow p - b - c$$

$$p - x - c \wedge x - q - c \rightarrow p - q - c$$

Tenemos las hipótesis, luego concluimos $p - q - c$. ■

Hasta ahora no hemos usado el axioma **A8**. Una consecuencia elemental es la siguiente:

Teorema 3.8 *Existen al menos tres puntos distintos.*[1]

Demostración: El axioma **A8** nos da puntos a, b, c que cumplen

$$\neg a - b - c \land \neg b - c - a \land \neg c - a - b.$$

El teorema 3.5, 1) implica que tienen que ser distintos dos a dos. ■

El teorema siguiente usa el anterior, pero en realidad sólo requiere una hipótesis más débil que **A8**, a saber, la existencia de dos puntos distintos:

Teorema 3.9 $\bigvee c(a - b - c \land b \neq c)$.

Demostración: Consideremos dos puntos distintos u y v. Por **A4** existe un punto c tal que $a - b - c \land \overline{bc} \equiv \overline{uv}$, luego $b \neq c$ por **A3**. ■

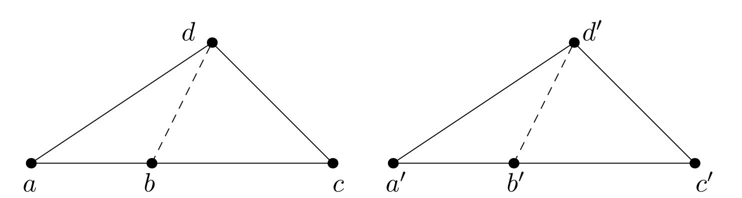
3.2.2 Más propiedades de la congruencia

Vamos a probar una variante de **A5** que parte de una *configuración interior de cinco segmentos,* definida como sigue:

$$\operatorname{Int}\begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} \leftrightarrow$$

$$a - b - c \land a' - b' - c' \land \overline{ac} \equiv \overline{a'c'} \land \overline{bc} \equiv \overline{b'c'} \land \overline{ad} \equiv \overline{a'd'} \land \overline{cd} \equiv \overline{c'd'}.$$

Teorema 3.10 $\operatorname{Int}\begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} \rightarrow \overline{bd} \equiv \overline{b'd'}$.

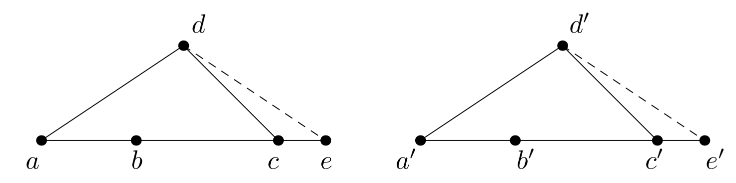


Demostración: Si $a = c$, como $\overline{ac} \equiv \overline{a'c'}$, también $a' = c'$, luego por **A6** tenemos que $b = c$ y $b' = c'$, luego la hipótesis $\overline{cd} \equiv \overline{c'd'}$ equivale a $\overline{bd} \equiv \overline{b'd'}$, que es lo que había que probar.

Podemos suponer, pues, que $a \neq c$. Por el teorema 3.9 existe un punto e tal que $a - c - e \land c \neq e$. Por **A4** existe un punto e' tal que $a' - c' - e' \land \overline{c'e'} \equiv \overline{ce}$.

[1]Sustituiremos los enunciados formales cuando sean más fáciles de asimilar en el lenguaje natural. Por ejemplo, el enunciado formal de este teorema sería:

$$\bigvee abc(a \neq b \land a \neq c \land b \neq c).$$



Es fácil ver que se cumple $\operatorname{Ext}\begin{pmatrix} a & c & e & d \\ a' & c' & e' & d' \end{pmatrix}$, y además $a \neq c$, luego podemos aplicar **A5** para concluir que $\overline{de} \equiv \overline{d'e'}$.

Sabemos que $a-b-c \wedge a-c-e$, luego 3.6, 2) nos da que $b-c-e$, e igualmente $b'-c'-e'$. Ahora es inmediato que se cumple $\operatorname{Ext}\begin{pmatrix} e & c & b & d \\ e' & c' & b' & d' \end{pmatrix}$, y además $e \neq c$, luego **A5** nos da que $\overline{bd} \equiv \overline{b'd'}$. ■

El teorema siguiente prueba que es posible definir una resta de segmentos:

Teorema 3.11 $a-b-c \wedge a'-b'-c' \wedge \overline{ac} \equiv \overline{a'c'} \wedge \overline{bc} \equiv \overline{b'c'} \rightarrow \overline{ab} \equiv \overline{a'b'}$.

Demostración: Basta observar que se cumple $\operatorname{Int}\begin{pmatrix} a & b & c & a \\ a' & b' & c' & a' \end{pmatrix}$, y así, por el teorema anterior $\overline{ab} \equiv \overline{a'b'}$. ■

Conviene introducir la notación siguiente:

$$(a,b,c) \equiv (a',b',c') \leftrightarrow \overline{ab} \equiv \overline{a'b'} \wedge \overline{ac} \equiv \overline{a'c'} \wedge \overline{bc} \equiv \overline{b'c'}.$$

Esto significa que las dos ternas de puntos determinan triángulos iguales (pero sin excluir el caso de que sean colineales).

Ahora podemos demostrar el análogo "interior" del axioma **A4**:

Teorema 3.12 $a-b-c \wedge \overline{ac} \equiv \overline{a'c'} \rightarrow \bigvee b'(a'-b'-c' \wedge (a,b,c) \equiv (a',b',c'))$.

Demostración: Por el teorema 3.9 existe un punto d' tal que $d'-a'-c'$, con $d' \neq a'$. Por **A4** existe un punto b' tal que $d'-a'-b' \wedge \overline{a'b'} \equiv \overline{ab}$, y a su vez un punto c'' tal que $d'-b'-c'' \wedge \overline{b'c''} \equiv \overline{bc}$.

d' a' b' c', c''

Vamos a probar que $c' = c''$. Por 3.6, 2) tenemos que $a'-b'-c'$ y $d'-a'-c''$, el teorema 3.3 nos da que $\overline{ac} \equiv \overline{a'c''}$ y el teorema 3.4 (con $q = d'$) nos da que $c'' = c'$, y entonces es claro que b' cumple lo requerido. ■

Terminamos con una relación notable entre las congruencias y la ordenación:

Teorema 3.13 $a-b-c \wedge (a,b,c) \equiv (a',b',c') \rightarrow a'-b'-c'$.

Demostración: Por el teorema anterior existe un punto b'' de manera que $a'-b''-c' \wedge (a,b,c) \equiv (a',b'',c')$. La transitividad de la congruencia nos da que $(a',b',c') \equiv (a',b'',c')$, y esto implica a su vez $\operatorname{Int}\begin{pmatrix} a' & b'' & c' & b'' \\ a' & b'' & c' & b' \end{pmatrix}$, luego el teorema 3.10 nos da que $\overline{b'b''} \equiv \overline{b''b''}$, luego por **A3** tiene que ser $b' = b''$, de donde $a'-b'-c'$. ■

3.2.3 Colinealidad

Tres puntos son colineales si están sobre la misma recta:

$$\mathrm{Col}(abc) \leftrightarrow b - a - c \vee a - b - c \vee a - c - b.$$

El teorema 3.5, 2) implica inmediatamente que esta relación no depende del orden de los puntos:

Teorema 3.14 $\mathrm{col}(abc) \to \mathrm{col}(acb) \wedge \mathrm{col}(bac) \wedge \mathrm{col}(bca) \wedge \mathrm{col}(cab) \wedge \mathrm{col}(cba)$.

Por 3.5, 1) tenemos además:

Teorema 3.15 $\mathrm{Col}(aab)$.

Como consecuencia inmediata de 3.13 tenemos:

Teorema 3.16 $\mathrm{Col}(abc) \wedge (a, b, c) \equiv (a', b', c') \to \mathrm{Col}(a'b'c')$.

Recíprocamente:

Teorema 3.17 $\mathrm{Col}(abc) \wedge \overline{ab} \equiv \overline{a'b'} \to \bigvee c' \, (a, b, c) \equiv (a', b', c')$.

Demostración: Supongamos en primer lugar $a - b - c$. Por **A4** existe un punto c' tal que $a' - b' - c' \wedge \overline{b'c'} \equiv \overline{bc}$, y por el teorema 3.3 también $\overline{ac} \equiv \overline{a'c'}$, luego $(a, b, c) \equiv (a', b', c')$.

Si $b - a - c$ el razonamiento es similar: tomamos un punto c' de manera que $b' - a' - c' \wedge \overline{a'c'} \equiv \overline{ac}$, el teorema 3.3 nos da que $\overline{bc} \equiv \overline{b'c'}$ y entonces $(a, b, c) \equiv (a', b', c')$.

Por último, si $a - c - b$ basta aplicar el teorema 3.12. ■

Diremos que ocho puntos forman una *configuración de cinco segmentos* si cumplen

$$\mathrm{Conf5}\begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} \leftrightarrow$$

$$\mathrm{Col}(abc) \wedge (a, b, c) \equiv (a', b', c') \wedge \overline{ad} \equiv \overline{a'd'} \wedge \overline{bd} \equiv \overline{b'd'}.$$

Como ilustración sirve la misma figura que ilustra el axioma **A5**, sólo que ahora los puntos a, b, c pueden estar ordenados de cualquier forma. El axioma **A5** y el teorema 3.10 se combinan ahora en el teorema siguiente:

Teorema 3.18 $\mathrm{Conf5}\begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} \wedge a \neq b \to \overline{cd} \equiv \overline{c'd'}$.

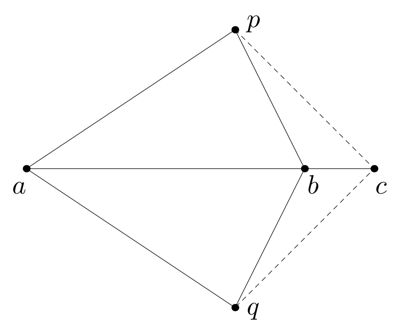
Demostración: Si $a - b - c$ tenemos $\mathrm{Ext}\begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} \wedge a \neq b$, luego basta aplicar **A5**.

Si $b - a - c$ tenemos $\mathrm{Ext}\begin{pmatrix} b & a & c & d \\ b' & a' & c' & d' \end{pmatrix} \wedge a \neq b$, y de nuevo concluimos por **A5**.

Si $a - c - b$ tenemos $\operatorname{Int}\begin{pmatrix} a & c & b & d \\ a' & c' & b' & d' \end{pmatrix}$, y aplicamos el teorema 3.10. ■

Conviene destacar el siguiente caso particular:

Teorema 3.19 $a \neq b \wedge \operatorname{Col}(abc) \wedge \overline{ap} \equiv \overline{aq} \wedge \overline{bp} \equiv \overline{bq} \to \overline{cp} \equiv \overline{cq}$.



Demostración: Basta observar que se cumple $\operatorname{Conf5}\begin{pmatrix} a & b & c & p \\ a & b & c & q \end{pmatrix}$ y aplicar el teorema anterior. ■

Ahora podemos probar la unicidad en el teorema 3.17:

Teorema 3.20 $a \neq b \wedge \operatorname{Col}(abc) \wedge \overline{ac} \equiv \overline{ac'} \wedge \overline{bc} \equiv \overline{bc'} \to c = c'$.

Demostración: Basta aplicar el teorema anterior con $p = c$ y $q = c'$. La conclusión es $\overline{cc} \equiv \overline{cc'}$, luego $c = c'$. ■

3.2.4 El teorema de conexión

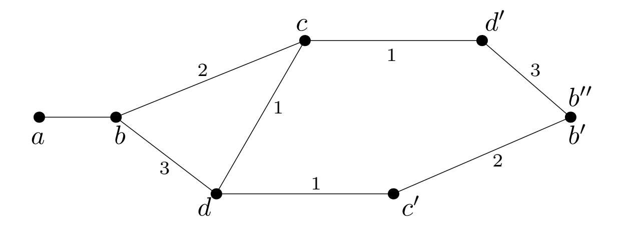
Finalmente demostramos un teorema cuyo contenido intuitivo es trivial, pero que no es fácil de deducir de los resultados que tenemos probados:

Teorema 3.21 $a \neq b \wedge a - b - c \wedge a - b - d \to a - c - d \vee a - d - c$.

Demostración: Por **A4** existen puntos c' y d' tales que $a - d - c' \wedge \overline{dc'} \equiv \overline{cd}$ y $a - c - d' \wedge \overline{cd'} \equiv \overline{cd}$. Basta probar que $c = c' \vee d = d'$.

Aplicando de nuevo **A4** existen puntos b' y b'' tales que $a - d' - b'' \wedge \overline{d'b''} \equiv \overline{bd}$ y $a - c' - b' \wedge \overline{c'b'} \equiv \overline{bc}$.

La situación es la que muestra la figura siguiente, en la que hemos bifurcado la recta para mostrar únicamente las relaciones que conocemos (números iguales señalan segmentos congruentes):



Demostraremos que $b' = b''$, como indica la figura. El teorema 3.6 2) nos da:

$$a - c - d' \wedge a - d' - b'' \to c - d' - b'', \qquad a - b - d \wedge a - d - c' \to b - d - c',$$

y el teorema 3.3 implica entonces que $\overline{cb''} \equiv \overline{bc'}$. Igualmente:

$a - d - c \wedge a - d' - b'' \to a - c - b''$ y esto, junto a $a - b - c$, implica $b - c - b''$.

$a - b - d \wedge a - d - c' \to a - b - c'$, y esto, junto a $a - c' - b'$, implica $b - c' - b'$.

El teorema 3.3 nos da que $\overline{bb''} \equiv \overline{bb'}$.

$a - b - d \wedge a - d - c' \to a - b - c'$, y esto, junto a $a - c' - b'$ implica $a - b - b'$.

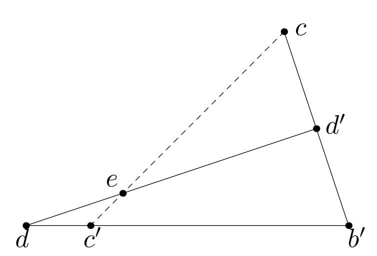
$a - b - c \wedge a - c - b'' \to a - b - b''$, y el teorema 3.4 implica que $b' = b''$.

Ahora es inmediato que se cumple $\operatorname{Ext}\begin{pmatrix} b & c & d' & c' \\ b' & c' & d & c \end{pmatrix}$.

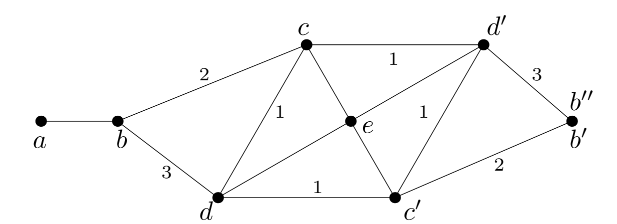
Podemos suponer que $b \neq c$, pues en caso contrario la hipótesis $a - b - d$ equivale a $a - c - d$, que es lo que hay que probar. Por lo tanto podemos aplicar **A5** y obtenemos que $\overline{c'd'} \equiv \overline{cd}$. Aplicamos de nuevo el teorema 3.6, 2):

$$a - c' - b' \wedge a - d - c' \to d - c' - b', \qquad a - c - b' \wedge a - c - d' \to c - d' - b'.$$

Esto nos permite aplicar **A7** a la situación que muestra la figura:



La conclusión es que existe un punto e tal que $d - e - d' \wedge c - e - c'$. En total tenemos la situación siguiente:



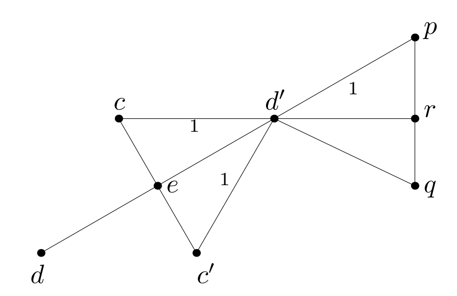
Es inmediato comprobar que se cumplen las configuraciones

$$\operatorname{Int}\begin{pmatrix} d & e & d' & c \\ d & e & d' & c' \end{pmatrix}, \quad \operatorname{Int}\begin{pmatrix} c & e & c' & d \\ c & e & c' & d' \end{pmatrix},$$

que nos dan respectivamente las congruencias $\overline{ce} \equiv \overline{ec'}$, $\overline{de} \equiv \overline{ed'}$.

Supongamos que $d \neq d'$ y vamos a probar que $c = c'$. Como los cuatro segmentos marcados con un 1 en la figura son congruentes, tiene que ser $c \neq d'$, o de lo contrario $c = d' = c' = d$. Aplicamos tres veces **A4** para obtener puntos p, r, q que cumplen:

$$d - d' - p \wedge \overline{d'p} \equiv \overline{cd'}, \quad c - d' - r \wedge \overline{d'r} \equiv \overline{d'e}, \quad p - r - q \wedge \overline{rq} \equiv \overline{rp}.$$



Se comprueba inmediatamente la configuración

$$\mathrm{Ext}\begin{pmatrix} c & d' & r & p \\ p & d' & e & c \end{pmatrix}$$

y, como $c \neq d$, el axioma **A5** nos da que $\overline{pr} \equiv \overline{ce}$, luego también $\overline{rq} \equiv \overline{ec'}$. A su vez, esto nos da la configuración

$$\mathrm{Ext}\begin{pmatrix} c & e & c' & d' \\ p & r & q & d' \end{pmatrix}.$$

Podemos suponer que $c \neq e'$, pues en caso contrario $c = c'$, que es lo que queremos probar. Así, el axioma **A5** nos da que $\overline{d'c'} \equiv \overline{d'q}$, luego $\overline{d'p} \equiv \overline{d'q}$.

Ahora usamos repetidamente el teorema 3.19. Para la primera aplicación tenemos en cuenta que $d' \neq r$, pues en caso contrario $d' = e = d$:

$$\begin{array}{l}
d' \neq r \wedge \mathrm{Col}(cd'r) \wedge \overline{d'p} \equiv \overline{d'q} \wedge \overline{rp} \equiv \overline{rq} \rightarrow \overline{cp} \equiv \overline{cq} \\
c \neq d' \wedge \mathrm{Col}(cd'b) \wedge \overline{cp} \equiv \overline{cq} \wedge \overline{d'p} \equiv \overline{d'q} \rightarrow \overline{bp} \equiv \overline{bq} \\
b \neq c \wedge \mathrm{Col}(bcb') \wedge \overline{bp} \equiv \overline{bq} \wedge \overline{cp} \equiv \overline{cq} \rightarrow \overline{b'p} \equiv \overline{b'q} \\
b \neq b' \wedge \mathrm{Col}(bdb') \wedge \overline{bp} \equiv \overline{bq} \wedge \overline{b'p} \equiv \overline{b'q} \rightarrow \overline{dp} \equiv \overline{dq} \\
b \neq b' \wedge \mathrm{Col}(bd'b') \wedge \overline{bp} \equiv \overline{bq} \wedge \overline{b'p} \equiv \overline{b'q} \rightarrow \overline{d'p} \equiv \overline{d'q} \\
d \neq d' \wedge \mathrm{Col}(dd'p) \wedge \overline{dp} \equiv \overline{dq} \wedge \overline{d'p} \equiv \overline{d'q} \rightarrow \overline{pp} \equiv \overline{pq}
\end{array}$$

de donde concluimos que $p = q$ y, como $\overline{pq} \equiv \overline{cc'}$, resulta que $c = c'$. ∎

Sin más que aplicar el teorema 3.6, b) a la conclusión del teorema anterior obtenemos:

Teorema 3.22 $a \neq b \wedge a - b - c \wedge a - b - d \rightarrow b - c - d \vee b - d - c.$

Por último probamos la versión "interior" del teorema de conexión:

Teorema 3.23 $a - b - d \wedge a - c - d \rightarrow a - b - c \vee a - c - b$.

DEMOSTRACIÓN: Por el teorema 3.9 existe p tal que $p - a - d \wedge p \neq a$. Por el teorema 3.6, 1) se cumple $p - a - b \wedge p - a - c$, luego por el teorema anterior $a - b - c \vee a - c - b$. ■

3.2.5 Lugares geométricos

En la geometría de Tarski podemos hablar de clases tal y como se explica en general, para cualquier teoría axiomática, en la sección 1.1. En el contexto de la geometría es costumbre llamar a las clases *lugares geométricos.*

A la clase universal la llamaremos el *espacio,* y la representaremos por

$$E = \{x \mid x = x\}.$$

Otro ejemplo de lugar geométrico es el *segmento* de extremos a y b, definido como

$$\overline{ab} = \{x \mid a - x - b\}.$$

Así, la expresión $x \in \overline{ab}$, no es sino una forma alternativa de escribir $a-x-b$. He aquí algunos resultados elementales que podemos expresar en términos de segmentos considerados como lugares geométricos:

Teorema 3.24 *Se cumple:*

1. $\overline{ab} = \overline{ba}$,
2. $\overline{aa} = \{a\}$,
3. $\{a, b\} \subset \overline{ab}$,
4. $\overline{ab} = \overline{cd} \leftrightarrow (a = c \wedge b = d) \vee (a = d \wedge b = c)$.

DEMOSTRACIÓN: 1) y 3) son consecuencia inmediata del teorema 3.5, mientras que 2) se sigue de **A6**. Para probar 4) suponemos $\overline{ab} = \overline{cd}$. Por 3) deducimos las relaciones

$$a - c - b, \qquad a - d - b, \qquad c - a - d, \qquad c - b - d.$$

Si $a \neq c$ aplicamos el teorema 3.6, 3):

$$a - b - c \wedge b - c - d \wedge b \neq c \rightarrow a - c - d \wedge a - b - d$$

$$d - a - c \wedge a - c - b \wedge a \neq c \rightarrow d - c - b \wedge d - a - b$$

Combinando la conclusión con $d - b - c \wedge a - d - b$, el teorema 3.5, 3) nos da $b = c \wedge a = d$.

Si, por el contrario, suponemos que $a = c$, entonces $c - d - b \wedge c - b - d$, luego $b = d$. La implicación opuesta es muy sencilla. ■

La última propiedad del teorema anterior afirma que un segmento determina sus extremos (salvo el orden), es decir, que un mismo segmento S sólo puede expresarse de dos formas: $S = \overline{ab}$ o $S = \overline{ba}$, para un par de puntos a y b unívocamente determinados por S (aunque las dos formas serán una sola si se da el caso $a = b$).

Por consiguiente, podemos hablar de segmentos S y T sin necesidad de explicitar sus extremos y escribir, por ejemplo, $S \equiv T$ en el sentido de que $S = \overline{ab}$, $T = \overline{cd}$ y $\overline{ab} \equiv \overline{cd}$. Aquí tenemos en cuenta que la congruencia no se altera si cambiamos $\overline{ab}$ por $\overline{ba}$ o $\overline{cd}$ por $\overline{dc}$.

De este modo, aunque técnicamente la congruencia es un relator que requiere cuatro puntos como argumentos, podemos pensar que determina una relación binaria sobre la clase de todos los segmentos.

Ejercicio: Probar que si $a - b - c$ entonces $\overline{ac} = \overline{ab} \cup \overline{bc}$ y $\overline{ab} \cap \overline{bc} = \{b\}$.

3.3 Ordenación de segmentos

Ya podemos ordenar los segmentos según su longitud:

Definición 3.25 $\overline{ab} \leq \overline{cd} \leftrightarrow \bigvee y(c - y - d \wedge \overline{ab} \equiv \overline{cy})$.

La interpretación geométrica es obvia: $\overline{ab}$ es más corto que $\overline{cd}$ si $\overline{cd}$ se puede cortar hasta un segmento congruente con $\overline{ab}$. Esto equivale a que $\overline{ab}$ se pueda prolongar hasta un segmento congruente con $\overline{cd}$:

Teorema 3.26 $\overline{ab} \leq \overline{cd} \leftrightarrow \bigvee x(a - b - c \wedge \overline{ac} \equiv \overline{cd})$.

Demostración: Supongamos que $\overline{ab} \leq \overline{cd}$ y sea y según la definición, es decir, tal que $c - y - d \wedge \overline{ab} \equiv \overline{cy}$. Por el teorema 3.17 existe un punto x tal que $(c, y, d) \equiv (a, b, x)$ y por el teorema 3.13 se cumple $a - b - x$ (y obviamente $\overline{ax} \equiv \overline{cd}$).

Recíprocamente, si existe un punto x tal que $a - b - c \wedge \overline{ax} \equiv \overline{cd}$, por el teorema 3.17 existe un punto y tal que $(a, x, b) \equiv (c, d, y)$ y por el teorema 3.13 se cumple $c - y - d$ (y obviamente $\overline{ab} \equiv \overline{cy}$), luego $\overline{ab} \leq \overline{cd}$. ■

Nota Técnicamente la relación $\overline{ab} \leq \overline{cd}$ es una fórmula del lenguaje de la geometría de Tarski con cuatro variables libres, pero podemos pensar que determina una relación binaria sobre la clase de todos los segmentos exactamente en el mismo sentido en que observamos esto de la relación de congruencia en la sección anterior. ■

Otro hecho elemental es que la relación de orden es compatible con la congruencia de segmentos en el sentido siguiente:

Teorema 3.27 $\overline{ab} \leq \overline{cd} \wedge \overline{ab} \equiv \overline{a'b'} \wedge \overline{cd} \equiv \overline{c'd'} \rightarrow \overline{a'b'} \leq \overline{c'd'}$.

Demostración: Sea y tal que $c - y - d \wedge \overline{ab} \equiv \overline{cy}$. Por el teorema 3.17 existe un punto y' tal que $(c, d, y) \equiv (c', d', y')$, y por el teorema 3.13 se cumple $c' - y' - d'$, y además $\overline{a'b'} \equiv \overline{ab} \equiv \overline{cy} \equiv \overline{c'y'}$, luego $\overline{a'b'} \leq \overline{c'd'}$. ■

El teorema siguiente recoge otras propiedades básicas de esta relación:

Teorema 3.28 *Se cumple:*

1. $\overline{ab} \leq \overline{ab}$,
2. $\overline{ab} \leq \overline{cd} \wedge \overline{cd} \leq \overline{ab} \rightarrow \overline{ab} \equiv \overline{cd}$,
3. $\overline{ab} \leq \overline{cd} \wedge \overline{cd} \leq \overline{ef} \rightarrow \overline{ab} \leq \overline{ef}$,
4. $\overline{aa} \leq \overline{cd}$,
5. $\overline{ab} \leq \overline{cd} \vee \overline{cd} \leq \overline{ab}$.

Demostración: Vamos a probar únicamente 2) y 5). Las otras propiedades se prueban sin dificultad.

Como $\overline{ab} \leq \overline{cd}$, existe un punto y tal que $c - y - d \wedge \overline{ab} \equiv \overline{cy}$. Como $\overline{cd} \leq \overline{ab}$, por el teorema 3.26 existe un x tal que $c - d - x \wedge \overline{ab} \equiv \overline{cx}$. Por 3.6, 2) tenemos que $c - y - d \wedge c - d - x \rightarrow c - y - x \wedge y - d - x$. Por el teorema 3.11:

$$a - b - b \wedge c - y - x \wedge \overline{ab} \equiv \overline{cx} \wedge \overline{ab} \equiv \overline{cy} \rightarrow \overline{bb} \equiv \overline{yx},$$

luego $y = x$ y, como $y - d - x$, el axioma **A6** nos da que $y = d$, luego $\overline{ab} \equiv \overline{cy} \equiv \overline{cd}$.

La propiedad 5) es fácil de probar, pero mostramos la demostración para destacar que se apoya en el teorema 3.22, que a su vez se prueba a partir del teorema de conexión, que no ha sido nada fácil de demostrar:

Dados dos puntos a y b, por el teorema 3.9 existe p tal que $p - a - b \wedge p \neq a$. Por **A4** existe un x tal que $p - a - x \wedge \overline{ax} \equiv \overline{cd}$. Por el teorema 3.22 tenemos

$$p - a - b \wedge p - a - x \rightarrow a - b - x \vee a - x - b,$$

y es claro que esto implica $\overline{ab} \leq \overline{cd} \vee \overline{cd} \leq \overline{ab}$. ■

Por último demostramos que la relación de orden determina la relación de ordenación:

Teorema 3.29 $\mathrm{Col}(abc) \rightarrow (a - b - c \leftrightarrow \overline{ab} \leq \overline{ac} \wedge \overline{bc} \leq \overline{ac})$.

Demostración: Si $a - b - c$, entonces se cumple $\overline{ab} \leq \overline{ac} \wedge \overline{bc} \leq \overline{ac}$ sin más que tomar $y = b$ en la definición.

Si se cumple $\overline{ab} \leq \overline{ac} \wedge \overline{bc} \leq \overline{ac}$, pero no $a - b - c$, entonces $a - c - b \vee b - a - c$. Suponemos el primer caso, pues el segundo se trata igualmente. Por la parte ya probada, $\overline{ac} \leq \overline{ab}$, luego por la antisimetría $\overline{ab} \equiv \overline{ac}$. Por el teorema 3.11:

$$a - c - b \wedge a - c - c \wedge \overline{ac} \equiv \overline{ac} \wedge \overline{ab} \equiv \overline{ac} \rightarrow \overline{cb} \equiv \overline{cc},$$

luego $b = c$, luego $a - b - c$, en contradicción con lo supuesto. ■

Conviene definir la relación de orden estricto:

$$\overline{ab} < \overline{cd} \leftrightarrow \overline{ab} \leq \overline{cd} \land \neg \overline{ab} \equiv \overline{cd},$$

cuyas propiedades se deducen trivialmente de las de la relación de orden no estricta.

3.4 Rectas

Antes de introducir el concepto de recta conviene estudiar una relación de equivalencia que esencialmente recoge la idea de que todo punto de una recta la divide en dos mitades:

3.4.1 La relación "estar al mismo lado de un punto"

Definición 3.30 Diremos que dos puntos a y b *están al mismo lado* de un punto p si cumplen:

$$a \sim_p b \leftrightarrow a \neq p \land b \neq p \land (p - a - b \lor p - b - a).$$

Vamos a dar varias caracterizaciones de esta relación. La primera dice que equivale a que los puntos p, a, b sean colineales, pero que p no esté en medio:

Teorema 3.31 $a \sim_p b \leftrightarrow \mathrm{Col}(apb) \land \neg a - p - b.$

Demostración: Si $a \sim_p b$, entonces $p - a - b \lor p - b - a$. Si fuera $a - p - b$ el teorema 3.5 nos daría que $a = p \lor b = p$, en contradicción con la definición de $a \sim_p b$. La implicación opuesta se sigue inmediatamente de las definiciones y del teorema 3.5. ■

Teorema 3.32 $a \neq p \land b \neq p \land c \neq p \land a - p - c \rightarrow (a \sim_p b \leftrightarrow b - p - c).$

Demostración: Tenemos que a y c están en lados opuestos respecto de p, y se trata de probar que los puntos que están al mismo lado que a son exactamente los que están al lado opuesto a c.

Si se cumple $a \sim_p b$, entonces $p - a - b \lor p - b - a$. En ambos casos llegamos a la misma conclusión:

$b - a - p \land a - p - c \rightarrow b - p - c$ por el teorema 3.6, 3).
$a - b - p \land a - p - c \rightarrow b - p - c$ por el teorema 3.6, 2).

Para la implicación contraria basta usar el teorema 3.22:

$c - p - a \land c - p - b \rightarrow p - a - b \lor p - b - a$, y esto implica $a \sim_p b$. ■

Una variante de la misma idea:

Teorema 3.33 $a \sim_p b \leftrightarrow a \neq p \land b \neq p \land \bigvee c(c \neq p \land a - p - c \land b - p - c).$

Demostración: Si $a \sim_p b$, tenemos por definición las desigualdades $a \neq p \land b \neq p$. Por el teorema 3.9 existe un punto c tal que $a - p - c \land p \neq c$, luego $a \neq c$, por **A6**. El teorema anterior nos da que $b - p - c$. La implicación contraria es consecuencia inmediata del teorema anterior. ■

La relación que estamos considerando es una relación de equivalencia:

Teorema 3.34 *Se cumple:*

1. $a \neq p \rightarrow a \sim_p a$,
2. $a \sim_p b \rightarrow b \sim_p a$,
3. $a \sim_p b \land b \sim_p c \rightarrow a \sim_p c$.

Demostración: Probamos únicamente la transitividad, pues las otras propiedades son inmediatas. Por el teorema 3.9, existe un x tal que $a-p-x \land x \neq p$. Entonces, como $a \sim_p b$, el teorema 3.32 implica que $b - p - x$ (el punto b está en el lado opuesto a x, como a), y aplicando de nuevo dicho teorema a $b - p - x \land b \sim_p c$ obtenemos que $c - p - x$. Por último el teorema anterior nos da que $c - p - x \land a - p - x \rightarrow a \sim_p c$. ■

Veamos ahora una variante del teorema 3.4:

Teorema 3.35 $r \neq a \land b \neq c \rightarrow \overset{1}{\bigvee} x(x \sim_a r \land \overline{ax} \equiv \overline{bc})$.

Demostración: Por el teorema 3.9 existe p tal que $p - a - r \land p \neq a$. Por **A4** existe un x tal que $p - a - x \land \overline{ax} \equiv \overline{bc}$.

Como $p - a - x \land p - a - r$, el teorema 3.33 nos da que $x \sim_a r$. Esto prueba la existencia. Si un punto x' cumple lo mismo, entonces $x \sim_a x'$, y por 3.32 tenemos $p - a - x'$, luego $x = x'$ por el teorema 3.4. ■

Ahora refinamos la condición de antisimetría de la ordenación de segmentos:

Teorema 3.36 $a \sim_p b \land \overline{pa} \leq \overline{pb} \land \overline{pb} \leq \overline{pa} \rightarrow a = b$.

Demostración: En principio sabemos que $\overline{pa} \equiv \overline{pb}$, y por el teorema anterior $a = b$. ■

Por último probamos:

Teorema 3.37 $a \sim_p b \rightarrow (\overline{pa} \leq \overline{pb} \leftrightarrow p - a - b)$.

Demostración: Si $p - a - b$ tenemos que $\overline{pa} \leq \overline{pb}$ por el teorema 3.29. Si $\overline{pa} \leq \overline{pb}$, tenemos que $a \sim_p b \rightarrow p-a-b \lor p-b-a$, pero si se da el caso $p-b-a$ entonces $\overline{pb} \leq \overline{pa}$ por la parte ya probada, luego $a = b$ por el teorema anterior y también $p - a - b$. ■

3.4.2 Rectas y semirrectas

Ya podemos definir las rectas como lugares geométricos:

Definición 3.38 Para cada par de puntos p, q definimos el lugar geométrico

$$pq = \{x \mid (p \neq q \land \mathrm{Col}(xpq)) \lor (x = p = q)\}.$$

Así, si $p = q$ tenemos que $pq = \{p\}$. Llamaremos *rectas* a los lugares geométricos de la forma pq con $p \neq q$.

Observemos que trivialmente se cumple

$$p \in pq \land q \in pq \land pq = qp.$$

Llamaremos *semirrectas* a los lugares geométricos de la forma

$$\overrightarrow{pq} = \{x \mid x \sim_p q\},$$

con $p \neq q$. Observemos que $\overrightarrow{pp} = \varnothing$.

Teorema 3.39 $p \neq q \land p \neq s \rightarrow (\overrightarrow{pq} = \overrightarrow{ps} \leftrightarrow q \sim_p s)$.

Demostración: El enunciado es una abreviatura de la fórmula siguiente:

$$p \neq q \land p \neq s \rightarrow (\bigwedge x(x \sim_p q \leftrightarrow x \sim_p s) \leftrightarrow q \sim_p s).$$

Y esto es consecuencia inmediata de que $\sim_p$ es una relación de equivalencia. ■

Teorema 3.40 $p \neq q \land p \neq r \land q - p - r \rightarrow pq = \overrightarrow{pq} \cup \{p\} \cup \overrightarrow{pr}$.

Demostración: Tomemos $x \in pq$. Si $x = p$ trivialmente está en la unión. Supongamos, pues, que $x \neq p$. La hipótesis es $\mathrm{Col}(pqx)$, que por definición equivale a $p - q - x \lor p - x - q \lor x - p - q$. En los dos primeros casos se cumple $x \sim_p q$, luego $x \in \overrightarrow{pq}$, mientras que en el tercer caso $x \sim_p r$ por el teorema 3.32, luego $x \in \overrightarrow{pr}$. Esto prueba una inclusión. La otra es inmediata. ■

El teorema siguiente afirma que una recta está determinada por dos cualesquiera de sus puntos:

Teorema 3.41 $p \neq q \land a \neq b \land a \in pq \land b \in pq \rightarrow ab = pq$.

Demostración: Probaremos primero un caso particular:

$$p \neq q \land s \neq p \land s \in pq \rightarrow pq = ps.$$

En efecto, la hipótesis $s \in pq$ equivale a $\mathrm{Col}(pqs)$, que a su vez equivale a $s - p - q \lor p - s - q \lor p - q - s$. Si $s - p - q$ entonces $pq = \overrightarrow{pq} \cup \{p\} \cup \overrightarrow{ps} = ps$, donde hemos usado dos veces el teorema anterior.

En los otros dos casos se cumple que $s \sim_p q$, luego tomando un $r \neq p$ tal que $r - p - s$, se cumple también $r - p - q$ y $pq = \overrightarrow{pq} \cup \{p\} \cup \overrightarrow{pr} = \overrightarrow{ps} \cup \{p\} \cup \overrightarrow{pr} = ps$, donde hemos usado el teorema 3.39.

Pasamos ya a demostrar el teorema. Como $p \neq q$, tiene que ser $a \neq p \vee a \neq q$. Suponemos sin pérdida de generalidad que $a \neq q$. Entonces, por el teorema anterior, como $a \in pq$, se cumple $pq = aq$. Igualmente, como $b \in pq = aq$, resulta que $aq = ab$, luego $ab = aq = pq$. ■

En muchos resultados sobre rectas no importa cuáles son los dos puntos que las determinan y no hay inconveniente en hablar de rectas sin especificar dichos puntos. Para ello definimos $\mathcal{R}$ como el conjunto de todas las rectas, lo cual, dicho así, no significa nada en concreto, pero podemos precisarlo estableciendo que escribir $\bigwedge R \in \mathcal{R}(\cdots)$ deberá entenderse como $\bigwedge pq(p \neq q \rightarrow \cdots)$, donde los puntos suspensivos representan ahora la fórmula que resulta de reemplazar R por pq en la fórmula original. Similarmente se interpretan los cuantificadores $\bigvee R \in \mathcal{R}(\cdots)$ o $\overset{1}{\bigvee} R \in \mathcal{R}(\cdots)$. Por ejemplo, en estos términos el teorema anterior puede reformularse así:

Teorema 3.42 $\bigwedge R \in \mathcal{R}(a \neq b \wedge a \in R \wedge b \in R \rightarrow R = ab)$.

Similarmente, ahora podemos enunciar de este modo que por dos puntos distintos pasa una única recta:

Teorema 3.43 $a \neq b \rightarrow \overset{1}{\bigvee} R \in \mathcal{R}(a \in R \wedge b \in R)$.

DEMOSTRACIÓN: Si desarrollamos la unicidad, esto equivale a

$$\bigvee R \in \mathcal{R}(a \in R \wedge b \in R) \wedge \bigwedge RS \in \mathcal{R}(a \in R \wedge b \in R \wedge a \in S \wedge b \in S \rightarrow R = S).$$

La existencia es trivial. Basta tomar $R = ab$. La unicidad la da el teorema anterior, pues $R = ab = S$. ■

Un enunciado alternativo es que si dos rectas son distintas entonces tienen a lo sumo un punto en común.

Para terminar probamos que la colinealidad que hemos definido significa lo que debía significar:

Teorema 3.44 $\mathrm{Col}(abc) \leftrightarrow \bigvee R \in \mathcal{R}(a \in R \wedge b \in R \wedge c \in R)$.

DEMOSTRACIÓN: Si $\mathrm{Col}(abc)$, entonces $c \in ab$, luego basta tomar $R = ab$. Si se cumple el miembro derecho, entonces $R = ab$ por el teorema 3.42, luego $c \in ab$, luego $\mathrm{Col}(abc)$. ■

3.5 Simetrías puntuales

Para demostrar propiedades más sofisticadas de las rectas necesitamos estudiar el concepto de simetría puntual. Empezamos definiendo el concepto de punto medio de un segmento:

Definición 3.45 Diremos que m es el *punto medio* del segmento $\overline{ab}$ si cumple

$$M(amb) \leftrightarrow a - m - b \land \overline{am} \equiv \overline{mb}.$$

Obviamente se cumple $M(amb) \to M(bma)$ y $M(ama) \leftrightarrow m = a$.

Desgraciadamente, no estamos en condiciones de probar que cada segmento tiene un punto medio (lo probaremos en 3.66). De momento demostramos algo más fácil:

Teorema 3.46 $\overset{1}{\bigvee} p' \; M(pap')$.

Demostración: Si $p = a$ se cumple con $p' = a$, y la unicidad es clara. Supongamos, pues, que $p \neq a$. La existencia de p' la da **A4**. Para probar la unicidad suponemos $p - a - p' \land p - a - p'' \land \overline{p'a} \equiv \overline{pa} \land \overline{p''a} \equiv \overline{pa}$. Entonces $p' \sim_a p''$ por el teorema 3.32 y $p' = p''$ por 3.35. ■

Definición 3.47 Definimos el *punto simétrico* de p respecto de a como el único punto $p' = S_a p$ que cumple $M(pap')$.

Los hechos siguientes son inmediatos:

$$S_a p = p' \leftrightarrow M(pap'), \qquad S_a S_a p = p,$$
$$\overset{1}{\bigvee} p \, S_a p = p', \qquad S_a p = p \leftrightarrow p = a.$$

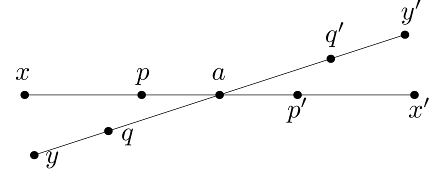
Ahora probamos que las simetrías son isometrías:

Teorema 3.48 $\overline{S_a p \, S_a q} \equiv \overline{pq}$.

Demostración: Llamemos $p' = S_a p$, $q' = S_a q$. Si $p = a$ entonces $p' = a$ y lo que hay que probar es que $\overline{aq} \equiv \overline{aq'}$, lo cual es cierto por definición de simetría. Suponemos, pues, que $p \neq a$.

Usando repetidamente **A4** podemos obtener puntos que cumplan:

$$p' - p - x \land \overline{px} \equiv \overline{qa}, \qquad x - p' - x' \land \overline{p'x'} \equiv \overline{qa},$$
$$q' - q - y \land \overline{qy} \equiv \overline{pa}, \qquad y - q' - y' \land \overline{q'y'} \equiv \overline{pa}.$$



Omitimos las aplicaciones rutinarias del teorema 3.6 que justifican que se cumplen todas las relaciones de ordenación que muestra la figura. Se comprueba $\mathrm{Ext}\begin{pmatrix} x & a & x' & y' \\ y' & a & y & x \end{pmatrix}$ y además $p \neq a$ implica $x \neq a$, luego por **A5** tenemos que $\overline{x'y'} \equiv \overline{xy}$. A su vez $\mathrm{Int}\begin{pmatrix} y & q & a & x \\ y' & q' & a & x' \end{pmatrix}$, luego $\overline{xq} \equiv \overline{x'q'}$. Igualmente $\mathrm{Int}\begin{pmatrix} x & p & a & q \\ x' & p' & a & q' \end{pmatrix}$, luego $\overline{pq} \equiv \overline{p'q'}$, como había que probar. ■

De aquí extraemos dos consecuencias inmediatas:

Teorema 3.49 *Se cumple:*

1. $p - q - r \to S_a p - S_a q - S_a r$,
2. $\overline{pq} \equiv \overline{rs} \to \overline{S_a p\, S_a q} \equiv \overline{S_a r\, S_a s}$.

1) se sigue del teorema 3.13, mientras que 2) se sigue de la transitividad de la congruencia.

Aunque seguimos sin estar en condiciones de probar la existencia del punto medio, al menos podemos probar su unicidad:

Teorema 3.50 $M(pap') \land M(pbp') \to a = b$.

Demostración: Por definición $p' = S_a p$. Por el teorema 3.48 tenemos que $\overline{pb} \equiv \overline{p'b} \equiv \overline{p\, S_a b}$, e igualmente $\overline{p'b} \equiv \overline{p'\, S_a b}$. Ahora el teorema 3.20 aplicado a $p - b - p'$ (con $c = b$ y $c' = S_a b$) nos da que $b = S_a b$, luego $a = b$. ■

Como consecuencia:

Teorema 3.51 $S_a p = S_b p \to a = b$.

Demostración: Tenemos que $M(paS_a p) = M(pbS_b p)$, luego basta aplicar el teorema anterior. ■

Veamos ahora que las simetrías no conmutan salvo en casos triviales:

Teorema 3.52 $S_a S_b p = S_b S_a p \leftrightarrow a = b$.

Demostración: Llamemos $p' = S_a p$. Si $S_a S_b p = S_b p'$, entonces se cumple $M(S_b p\, a\, S_b p')$. Como las simetrías conservan las congruencias y la ordenación, transforman puntos medios en puntos medios, luego aplicando S_b obtenemos $M(p\, S_b a\, p')$, pero también $M(pap')$, luego la unicidad del punto medio implica que $S_b a = a$, luego $a = b$. La implicación opuesta es trivial. ■

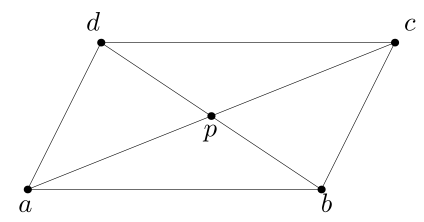
La condición de que el punto medio de dos puntos tiene que estar entre ellos es redundante salvo en casos triviales:

Teorema 3.53 $\mathrm{Col}(amb) \land \overline{ma} \equiv \overline{mb} \to a = b \lor M(amb)$.

DEMOSTRACIÓN: La colinealidad significa que $a-m-b \vee m-a-b \vee m-b-a$. En el primer caso se cumple la definición de $M(amb)$, en el segundo tenemos que $m-a-b \wedge m-b-b \rightarrow \overline{ab} \equiv \overline{bb}$ por el teorema 3.11, luego $a=b$. El tercer caso es análogo al segundo. ■

Probamos ahora dos resultados técnicos sobre puntos medios que necesitaremos más adelante. El primero viene a decir que las diagonales de un paralelogramo se cortan en su punto medio, pero no podemos enunciarlo así sin haber visto nada sobre paralelas:

Teorema 3.54 $\neg\mathrm{Col}(abc) \wedge b \neq d \wedge \overline{ab} \equiv \overline{cd} \wedge \overline{bc} \equiv \overline{da} \wedge \mathrm{Col}(apc) \wedge \mathrm{Col}(bpd) \rightarrow M(apc) \wedge M(bpd)$.



DEMOSTRACIÓN: Por el teorema 3.17 existe un punto p' de manera que $(b,d,p) \equiv (d,b,p')$. Así se cumple claramente $\mathrm{Conf5}\begin{pmatrix} b & d & p & a \\ d & b & p' & c \end{pmatrix}$. Como además suponemos que $b \neq d$, concluimos que $\overline{pa} \equiv \overline{p'c}$.

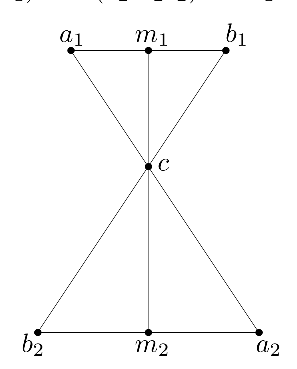
A su vez $\mathrm{Conf5}\begin{pmatrix} b & d & p & c \\ d & b & p' & a \end{pmatrix}$, luego $\overline{pc} \equiv \overline{p'a}$. Con esto tenemos que $(a,b,c) \equiv (c,p',a)$, luego el teorema 3.16 nos da $\mathrm{Col}(acp')$. Igualmente concluimos $\mathrm{Col}(bdp')$, pero entonces p y p' están en las rectas ac y bc, que son distintas, porque $\neg\mathrm{Col}(abc)$, luego $p=p'$. Por lo tanto $\overline{pa} \equiv \overline{pc}$ y, como $a \neq c$ (de nuevo porque $\neg\mathrm{Col}(abc)$), el teorema anterior nos da que $M(apc)$.

Por otra parte tenemos que $(b,d,p) \equiv (d,b,p)$, luego $\overline{dp} \equiv \overline{bp} \wedge d \neq b$ (si $d=b=p$, los puntos a,b,c serían colineales) y el teorema anterior implica también que $M(bpd)$. ■

El teorema siguiente es un poco más sofisticado:

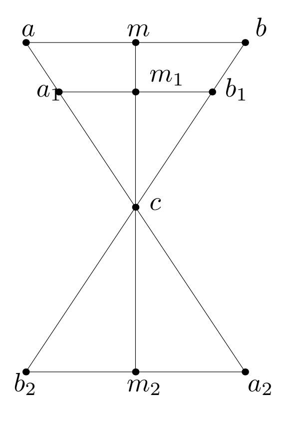
Teorema 3.55 $a_1 - c - a_2 \wedge b_1 - c - b_2 \wedge \overline{ca_1} \equiv \overline{cb_1} \wedge \overline{ca_2} \equiv \overline{cb_2} \wedge$

$$M(a_1 m_1 b_1) \wedge M(a_2 m_2 b_2) \rightarrow m_1 - c - m_2.$$



DEMOSTRACIÓN: Se cumple $\overline{ca_1} \leq \overline{ca_2} \vee \overline{ca_2} \leq \overline{ca_1}$. Por la simetría de las hipótesis no perdemos generalidad si suponemos que $\overline{ca_1} \leq \overline{ca_2}$.

Si $a_1 = c$, entonces $b_1 = c = m_1$ y la conclusión es trivial, así que podemos suponer que $a_1 \neq c$ y, en consecuencia, $a_2 \neq c$. Llamemos $a = S_c a_2$, $b = S_c b_2$. Entonces $m = S_c m_2$ cumple $M(bma)$.



Como $a_2 - c - a \wedge a_2 - c - a_1$, tenemos $a_2 \sim_c a$, luego $\overline{ca_1} \leq \overline{ca}$ implica que $c - a_1 - a$ por el teorema 3.37. Igualmente $c - b_1 - b$. El teorema 3.7 nos da un punto q tal que $m - q - c \wedge a_1 - q - b_1$. El teorema 3.6 nos da que $m - q - c \wedge m - c - m_2 \rightarrow q - c - m_2$.

Basta ver que $q = m_1$, pues entonces tenemos que $m_1 - c - m_2$, que es lo que hay que probar. Se comprueba Int $\begin{pmatrix} a & a_1 & c & m \\ b & b_1 & c & m \end{pmatrix}$, luego $\overline{ma_1} \equiv \overline{mb_1}$. El teorema 3.19 nos da:

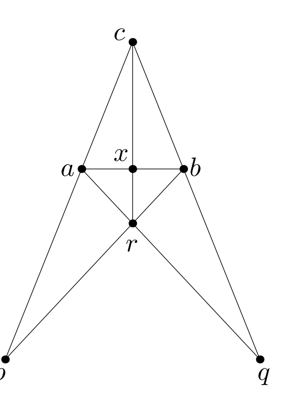
$$m \neq c \wedge m - q - c \wedge \overline{ma_1} \equiv \overline{mb_1} \wedge \overline{ca_1} \equiv \overline{cb_1}$$
$$\rightarrow \overline{qa_1} \equiv \overline{qb_1}.$$

Pero la hipótesis $m \neq c$ es superflua, pues si $m = c$ entonces $q = m$ y la conclusión es obvia. Por definición de punto medio, tenemos que $M(a_1 q b_1)$, pero también $M(a_1 m_1 b_1)$, luego por la unicidad $q = m_1$. ■

Finalmente demostramos la existencia del punto medio en el caso particular de dos puntos para los que exista un punto equidistante de ambos:

Teorema 3.56 $\overline{ca} \equiv \overline{cb} \rightarrow \bigvee x\, M(axb)$.

DEMOSTRACIÓN: Si Col(abc), el teorema 3.53 nos da que, o bien $a = b$, en cuyo caso sirve $x = a$, o bien $M(acb)$. Por lo tanto podemos suponer que a, b, c no son colineales.



Por el teorema 3.9 existe un punto p de manera que $c - a - p \wedge a \neq p$, por **A4** existe un punto q tal que $c - b - q \wedge \overline{bq} \equiv \overline{ap}$. La figura muestra estos puntos junto con otros dos puntos r y x que obtenemos por aplicaciones sucesivas de **A7**:

El punto r cumple $a - r - q \wedge b - r - p$, y se obtiene de aplicar **A7** al triángulo $\widehat{pcb}$: la recta aq corta al lado $\overline{pc}$, pero no a $\overline{pr}$, luego tiene que cortar a $\overline{pb}$.

El punto x cumple $a - x - b \wedge r - x - c$, y se obtiene de aplicar **A7** al triángulo $\widehat{pcr}$, pues la recta ab corta al lado $\overline{pc}$, pero no a $\overline{pr}$, luego tiene que cortar a $\overline{rc}$.

Ahora comprobamos Ext $\begin{pmatrix} c & a & p & b \\ c & b & q & a \end{pmatrix}$, luego $\overline{pb} \equiv \overline{qa}$. El teorema 3.17 nos da un punto r' tal que $(b, p, r) \equiv (a, q, r')$, y el teorema 3.13 nos da que

$a - r' - q$. Entonces $\mathrm{Int}\begin{pmatrix} b & r & p & a \\ a & r' & q & b \end{pmatrix}$, luego $\overline{ar} \equiv \overline{br'}$. A su vez se cumple $\mathrm{Int}\begin{pmatrix} b & r & p & q \\ a & r' & q & p \end{pmatrix}$, luego $\overline{qr} \equiv \overline{pr'}$. Tenemos entonces que $(a, r, q) \equiv (b, r', p)$ (aquí usamos que $(b, r, p) \equiv (a, r', q)$) y el teorema 3.16 implica $\mathrm{Col}(br'p)$.

Pero entonces r y r' están en las rectas aq y bp, que son distintas, pues si suponemos que son iguales llegamos a $\mathrm{Col}(abc)$, luego $r = r'$, luego $\overline{ra} \equiv \overline{rb}$. Por último el teorema 3.19 nos da que

$$r \neq c \land \mathrm{Col}(rxc) \land \overline{ra} \equiv \overline{rb} \land \overline{ca} \equiv \overline{cb} \rightarrow \overline{ax} \equiv \overline{xb}.$$

Para aplicar esto sólo falta comprobar que $r \neq c$, pero en caso contrario sería $x = c$ y $\mathrm{Col}(abc)$. Concluimos que $M(axb)$. ■

3.6 Perpendicularidad

Con ayuda de las simetrías puntuales podemos definir el concepto de ángulo recto, que a su vez nos permitirá definir la perpendicularidad entre rectas:

Definición 3.57 Diremos que tres puntos a, b, c forman un *ángulo recto* (de vértice b) si cumplen

$$Rabc \leftrightarrow \overline{ac} \equiv \overline{a\,S_bc}.$$

Veamos algunas propiedades elementales:

Teorema 3.58 *Se cumple:*

1. $Rabc \leftrightarrow Rcba$,
2. $Rabb$,
3. $Raba \rightarrow a = b$,
4. $Rabc \rightarrow RabS_bc$,
5. $Rabc \land a \neq b \land \mathrm{Col}(baa') \rightarrow Ra'bc$,
6. $Rabc \land \mathrm{Col}(abc) \rightarrow a = b \lor c = b$,
7. $Rabc \land Ra'bc \land a - c - a' \rightarrow b = c$.

Demostración: Notemos que 1) no es difícil de probar, pero no es trivial: el miembro izquierdo significa que $\overline{ac} \equiv \overline{a\,S_bc}$, mientras que el miembro derecho es $\overline{ac} \equiv \overline{c\,S_ba}$, pero el teorema 3.48 implica que $\overline{a\,S_bc} \equiv \overline{S_ba\,c}$, luego la equivalencia es clara.

2) es inmediata.

3) Por definición, $Raba$ es $\overline{aa} \equiv \overline{a\, S_b a}$, lo que equivale a que $a = S_b a$, y esto implica que $a = b$.

4) también es inmediata. Notemos que se interpreta como que el suplementario de un ángulo recto es recto.

5) Se interpreta como que $Rabc$ no depende de a, sino de la recta ab. La prueba es una aplicación obvia del teorema 3.19.

6) afirma que si tres puntos forman ángulo recto no pueden ser colineales salvo en los casos triviales. Si $a \neq b$ el apartado 5) nos da que $Rcbc$ y entonces 3) nos permite concluir $b = c$.

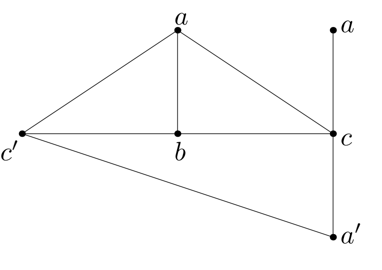
7) puede interpretarse como que un triángulo no puede tener un ángulo igual a dos rectos. El caso $a = a'$ es trivial, pues implica que $a = c$, luego $b = c$. Supongamos, pues, que $a \neq a'$. Si llamamos $c' = S_b c$, el teorema 3.20 nos da que

$$\overline{ac} \equiv \overline{ac'} \wedge \overline{a'c} \equiv \overline{a'c'} \wedge \mathrm{Col}(aca') \wedge a \neq a' \to c = c',$$

luego $b = c$. ■

Ahora demostramos que un triángulo no puede tener dos ángulos rectos:

Teorema 3.59 $Rabc \wedge Racb \to b = c$.



DEMOSTRACIÓN: En la figura hemos representado el punto a en dos sitios distintos porque la situación es imposible (salvo en el caso degenerado $b = c$). Llamamos $c' = S_b c$ y $a' = S_c a$.

De $Rabc$ se sigue que $\overline{ac} \equiv \overline{ac'}$, mientras que $Racb$ implica $Racc'$ por 3.58, 5) (suponiendo que $b \neq c$), luego $\overline{c'a} \equiv \overline{c'a'}$. Por consiguiente, $\overline{a'c} \equiv \overline{ac} \equiv \overline{ac'} \equiv \overline{a'c'}$, y esto significa que $Ra'bc$. Por 3.58, 7) tenemos que $Rabc \wedge Ra'bc \wedge a - c - a' \to b = c$. ■

Las isometrías conservan los ángulos rectos:

Teorema 3.60 $Rabc \wedge (a, b, c) \equiv (a', b', c') \to Ra'b'c'$.

DEMOSTRACIÓN: Si $b = c$, entonces $b' = c'$, luego $Ra'b'c'$. Por lo tanto podemos suponer que $b \neq c$. Llamemos $d = S_b c$ y $d' = S_{b'} c'$. Entonces es claro que $\mathrm{Ext}\begin{pmatrix} c & b & d & a \\ c' & b' & d' & a' \end{pmatrix}$, luego $\overline{ad} \equiv \overline{a'd'}$, luego $\overline{a'c'} \equiv \overline{ac} \equiv \overline{ad} \equiv \overline{a'd'}$, luego $Ra'b'c'$. ■

Ahora definimos el concepto de perpendicularidad de rectas:

Definición 3.61 Diremos que dos rectas son *perpendiculares* si se cortan en un punto x de modo que todo punto de una forma un ángulo recto de vértice x con todo punto de la otra. Formalmente:

$$ab \perp cd \leftrightarrow a \neq b \wedge c \neq d \wedge \bigvee x(x \in ab \wedge x \in cd \wedge \bigwedge u \in ab \bigwedge v \in cd\, Ruxv).$$

Observemos que una recta no puede ser perpendicular a sí misma, pues entonces tendríamos tres puntos colineales que formarían ángulo recto, en contra de 3.58, 6). Por consiguiente, el punto x de la definición es único, pues es necesariamente el punto de corte de las rectas.

En principio, la definición anterior es una propiedad de cuatro puntos, pero vemos que depende únicamente de las rectas que determinan dos pares de ellos, por lo que, cuando no sea relevante destacar ningún par de puntos de las rectas consideradas, podemos escribir $R \perp R'$. Por ejemplo, es inmediato que se cumple $R \perp R' \leftrightarrow R' \perp R$.

El teorema 3.58, 5) implica que para que dos rectas sean perpendiculares basta con que un punto de una (distinto del punto de intersección) forme ángulo recto con un punto de la otra:

Teorema 3.62 *Para todo par de rectas R y R', se cumple:*

$$R \perp R' \leftrightarrow \bigvee x(x \in R \cap R' \wedge \bigvee u \in R \bigvee v \in R'(u \neq x \wedge v \neq x \wedge Ruxv)).$$

Veamos ahora que por un punto exterior a una recta pasa una única perpendicular:

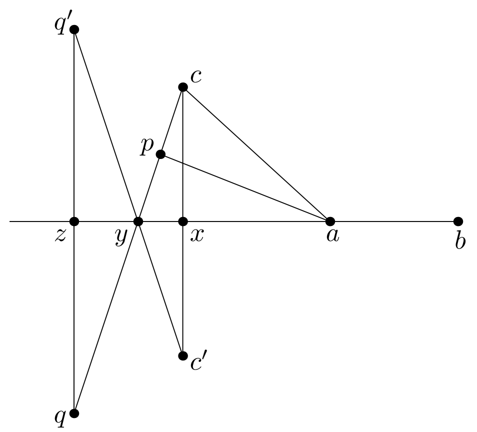
Teorema 3.63 $c \notin R \rightarrow \overset{1}{\bigvee} x \in R\ R \perp xc.$

DEMOSTRACIÓN: La unicidad se prueba fácilmente: si $x_1, x_2 \in R$ cumplen $R \perp x_1c \wedge R \perp x_2c$, entonces $Rcx_1x_2 \wedge Rcx_2x_1$, luego $x_1 = x_2$ por 3.59.

Para probar la existencia pongamos que $R = ab$, con $a \neq b$. Por **A4** existe un punto y tal que $y - a - b \wedge \overline{ay} \equiv \overline{ac}$. Por el teorema 3.56 existe un punto p tal que $M(ypc)$, luego $Rapy$.

Consideramos puntos que cumplan las condiciones siguientes:

$$a-y-z \wedge \overline{yz} \equiv \overline{yp}, \qquad p-y-q \wedge \overline{yq} \equiv \overline{ya}, \qquad q' = S_z q, \qquad q'-y-c' \wedge \overline{yc'} \equiv \overline{yc}.$$



Se comprueba inmediatamente

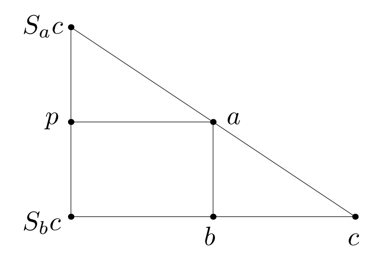
$$\text{Ext}\begin{pmatrix} a & y & z & q \\ q & y & p & a \end{pmatrix},$$

y como claramente $a \neq y$ (porque $c \notin R$), concluimos que $\overline{qz} \equiv \overline{ap}$, luego $(ap, p, y) \equiv (q, z, y)$, luego $Rapy \rightarrow Rqzy$ (por 3.60), luego $\overline{yq} \equiv \overline{yq'}$. Como $\overline{yc} \equiv \overline{yc'}$, el teorema 3.56 implica que el segmento $\overline{cc'}$ tiene punto medio, digamos x, de modo que $M(cxc')$, luego $Ryxc$. El teorema 3.55 implica que $z - y - x$. Por construcción $y, z \in R$, y además $y \neq z$, pues en caso contrario $c = p = y \in R$, luego $x \in R$, luego $cx \perp R$. ■

El punto x se llama *pie* de la perpendicular a R por c.

Para probar la existencia de perpendiculares por un punto de una recta necesitamos un resultado previo:

Teorema 3.64 $Rabc \wedge MS_a c\, p\, S_b c \rightarrow Rbap \wedge (b \neq c \rightarrow a \neq p)$.



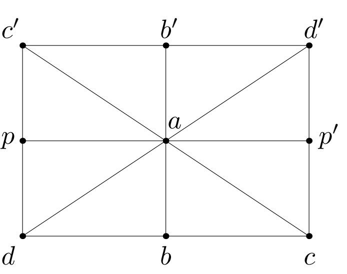
Demostración: Llamemos $c' = S_a c$, $d = S_b c$, $b' = S_a b$, $d' = S_a d$, $p' = S_a p$. Entonces $Rb'bc$, bien por el teorema 3.58, 5) o trivialmente si $a = b$. Esto implica que $\overline{b'c} \equiv \overline{b'd}$, luego aplicando S_a llegamos a que $\overline{bc'} \equiv \overline{bd'}$.

Es claro entonces que

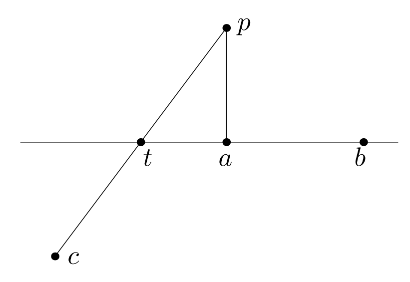
$$\mathrm{Int}\begin{pmatrix} c' & p & d & b \\ d' & p' & c & b \end{pmatrix},$$

luego $\overline{bp} \equiv \overline{bp'}$, y esto significa que $Rbap$.

Si $a = p$, entonces $c = S_a c' = S_p c' = d$, luego $b = d$. ■



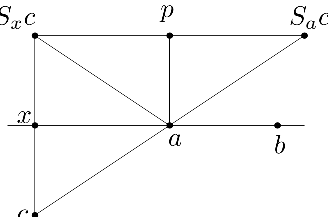
Teorema 3.65 $a \neq b \rightarrow \bigvee pt(ab \perp pa \wedge \mathrm{Col}(abt) \wedge c - t - p)$.



Aunque todavía no estamos en condiciones de enunciar esto, lo que afirma este teorema en el caso en el que a, b, c no son colineales es que existe una perpendicular a ab por a con la condición adicional de estar contenida en el plano abc. Más adelante (teorema 4.17) veremos que esta condición adicional hace que sea única.

Demostración: Supongamos en primer lugar $\neg\mathrm{Col}(abc)$. Sea $x \in ac$ el pie de la perpendicular a ab por c. Así $Raxc$, luego $\overline{a\, S_x c} \equiv \overline{ac} \equiv \overline{a\, S_a c}$. El teorema 3.56 nos da que existe un punto p tal que $MS_x c\, p\, S_a c$. El teorema anterior

implica entonces que $Rxap$ y, como $x \neq c$ (porque $x \in ab$ y $c \notin ab$), el teorema nos da también que $a \neq p$.



El teorema 3.7 implica que existe un t tal que $c - t - p \wedge x - t - a$. En particular $\mathrm{Col}(abt)$.

Si $x \neq a$, entonces, como $Rxap$, se cumple que $ab \perp pa$, mientras que si $x = a$ entonces $pa = pt = cx$, luego también $ab \perp pa$.

Consideremos ahora el caso en que $\mathrm{Col}(abc)$. Por **A8** podemos tomar un punto c' tal que $\neg\mathrm{Col}(abc')$ y por el caso ya probado existe un punto p tal que $ab \perp pa$. Basta tomar $t = c$. ■

Observemos que el teorema anterior es el único resultado en el que hasta ahora hemos empleado plenamente el axioma **A8**, es decir, la existencia de tres puntos no colineales. Los teoremas precedentes requerían a lo sumo la existencia de dos puntos distintos. Es lógico que así sea, pues el teorema anterior afirma en particular que toda recta tiene una perpendicular, y la existencia de dos rectas perpendiculares implica la existencia de tres puntos no colineales (que forman un ángulo recto). En cambio, es menos obvio que el teorema siguiente requiera también el axioma **A8**:

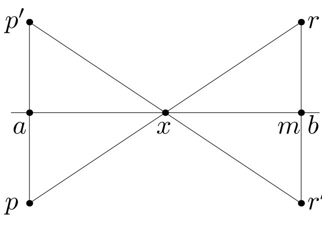
Teorema 3.66 $\overset{1}{\bigvee} x\ M(axb)$.

DEMOSTRACIÓN: La unicidad está probada en 3.50. Si $a = b$ el punto medio es $x = a$, luego podemos suponer que $a \neq b$.

El teorema anterior nos da un punto q tal que $bq \perp ab$ (necesariamente $q \notin ab$). Una segunda aplicación del teorema anterior (tomando ahora q como el punto c del enunciado) nos da que existe un punto p tal que $ap \perp ab$ y $p - t - q$, para cierto $t \in ab$.

Por la simetría en las hipótesis podemos suponer que $\overline{ap} \leq \overline{bq}$. Sea entonces r tal que $b - r - q$ y $\overline{ap} \equiv \overline{br}$. Por **A7** aplicado al triángulo $\widehat{tbq}$ existe un punto x tal que $t - x - b \wedge r - x - p$. En particular $x \in ab$.

Se cumple que $x \neq a$, pues en caso contrario $\mathrm{Col}(par)$, luego $ra = pa$ sería perpendicular a ab, al igual que $rb = qb$, y entonces 3.63 nos da que $a = b$, contradicción.



Sea $p' = S_a p$ y tomemos un punto r' tal que $p' - x - r' \wedge \overline{xr'} \equiv \overline{xr}$. El teorema 3.56 nos da que existe un punto m tal que $M(rmr')$. Entonces $Rrmx$. Por otra parte tenemos que $Rxap$ (porque $ap \perp ab$), luego $\overline{xp} \equiv \overline{xp'}$. Podemos aplicar el teorema 3.55, que nos da $a - x - m$, luego $m \in ax = ab$.

Así pues, las rectas rm y rb son ambas perpendiculares a ab, luego por 3.63 tiene que ser $m = b$. Así pues, $M(rbr')$ y $a - x - b$.

Basta probar que $\overline{bp} \equiv \overline{ar}$, pues entonces 3.54 nos da que $M(axb) \wedge M(pxr)$. Para ello usamos que

$$\mathrm{Int}\begin{pmatrix} p' & a & p & r \\ r & b & r' & p' \end{pmatrix},$$

luego $\overline{ra} \equiv \overline{p'b}$. Por otra parte, $Rbap$ implica que $\overline{bp} \equiv \overline{bp'}$, luego $\overline{bp} \equiv \overline{ar}$. ■

Conviene observar que en la prueba del teorema anterior hemos demostrado lo siguiente:

Teorema 3.67 $pa \perp ab \wedge qb \perp ab \wedge Col(abt) \wedge p - t - q \wedge b - r - q \wedge \overline{ap} \equiv \overline{br} \rightarrow \bigvee x(M(axb) \wedge M(pxr))$.

3.7 Planos

En esta sección definiremos los planos en la geometría de Tarski, pero previamente debemos introducir y estudiar dos nuevos conceptos. El primero será una relación análoga a $a - b - c$ en la que el punto central se sustituye por una recta, el segundo será la relación "estar al mismo lado de una recta" análoga a la relación "estar al mismo lado de un punto", que hemos usado para definir las rectas.

3.7.1 Separación de puntos por rectas

Definición 3.68 Diremos que una recta pq separa a dos puntos a y b si corta al segmento $\overline{ab}$, es decir:

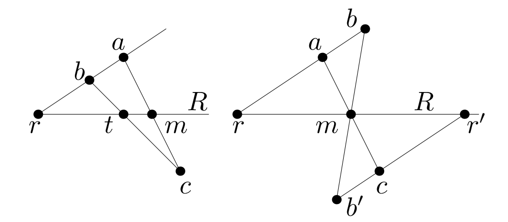
$$a - pq - b \leftrightarrow p \neq q \wedge a \notin pq \wedge b \notin pq \wedge \bigvee t(t \in pq \wedge a - t - b).$$

En principio, acabamos de definir una relación que involucra a cuatro puntos, pero vemos que no depende directamente de p y de q, sino de la recta pq, por lo que cuando no necesitemos especificar estos puntos escribiremos $a - R - b$, donde R representa una recta. Es inmediato que $a - R - b \leftrightarrow b - R - a$.

Para obtener las propiedades básicas de este concepto de separación necesitamos dos resultados técnicos. Luego veremos que la hipótesis sobre el punto medio en el teorema siguiente es innecesaria:

Teorema 3.69 $a - R - c \wedge m \in R \wedge M(amc) \wedge r \in R \rightarrow \bigwedge b(a \sim_r b \rightarrow b - R - c)$.

DEMOSTRACIÓN: Si $a \sim_r b$, entonces $r - b - a \vee r - a - b$.

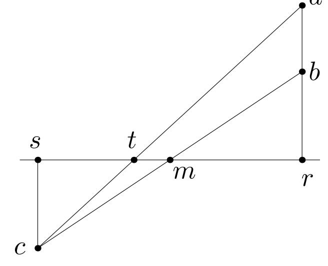


Si $r - b - a$ aplicamos el axioma **A7** al triángulo $\widehat{ram}$, con lo que existe un punto t tal que $b - t - c \wedge m - t - r$, y esto implica que $b - R - c$.

Si $r - a - b$ llamamos $b' = S_m b$ y $r' = S_m r$, con lo que $r' - c - b'$ y, por el caso ya probado, como $b' - R - b \wedge M(b'mb)$, se cumple $c - R - b$. ∎

Teorema 3.70 *Supongamos* $a - R - c \wedge r \in R \wedge R \perp ar \wedge s \in R \wedge R \perp cs$. *Entonces:*

1. $M(rms) \rightarrow \bigwedge u(u \sim_r a \leftrightarrow S_m u \sim_s c)$,
2. $\bigwedge uv(u \sim_r a \wedge v \sim_s c \rightarrow u - R - v)$.



DEMOSTRACIÓN: Tomemos $t \in R$ tal que $a - t - c$. Supongamos en primer lugar que $r \neq s$ (con lo que $t \neq r$). Por la simetría de las hipótesis podemos suponer que $\overline{sc} \leq \overline{ra}$, con lo que existe un punto b tal que $r - b - a \wedge \overline{rb} \equiv \overline{sc}$.

1) Aplicamos **A7** al triángulo $\widehat{art}$, que nos da que $\overline{bc}$ corta a $\overline{rt}$, luego a R. Esto nos sitúa en las hipótesis del teorema 3.67, luego existe un punto m tal que $M(rms) \wedge M(bmc)$. Por la unicidad del punto medio, se trata del punto m del enunciado.

Como $a \sim_r b$, tenemos que $u \sim_r a \leftrightarrow u \sim_r b \leftrightarrow S_m u \sim_s c$, pues el teorema 3.49, 1) implica que S_m transforma la relación $\sim_r$ en $\sim_s$ y viceversa.

2) Supongamos $u \sim_r a$, $v \sim_s c$. Por 1) tenemos que $u' = S_m u \sim_s c$, luego $u' \sim_s v$.

Como $u' - R - u \wedge M(umu') \wedge u' \sim_s v$, el teorema anterior nos da $v - R - u$.

Supongamos ahora que $r = s$, con lo que $ac = ar = cs$, luego $t = r = s = m$, ya que t y r son ambos el punto de corte de R y ac. El teorema se reduce a:

$$\bigwedge u(u \sim_t a \leftrightarrow S_t u \sim_t c) \wedge \bigwedge uv(u \sim_t a \wedge v \sim_t c \rightarrow u - R - v),$$

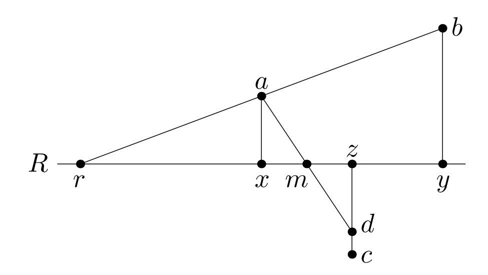
y esto es consecuencia de los hechos que conocemos sobre separación de puntos por puntos en una recta. Por ejemplo, 3.40 nos da que $ac = \overrightarrow{ta} \cup \{t\} \cup \overrightarrow{tc}$, Si $u \sim_t a$, como $\neg u \sim_t S_t u$, tiene que ser $S_t u \sim_t c$, e igualmente se prueba la implicación contraria.

Si $u \sim_t a \wedge v \sim_t c$, entonces $\neg u \sim_t v$, luego $u - t - v$, luego $u_R - v$. ∎

Finalmente podemos probar un resultado sin hipótesis redundantes:

Teorema 3.71 $a - R - c \wedge r \in R \rightarrow \bigwedge b(a \sim_r b \rightarrow b - R - c)$.

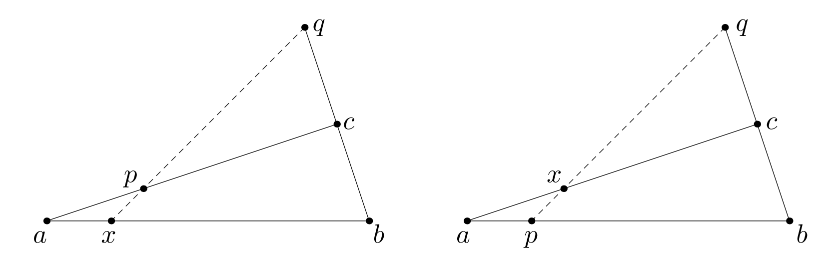
DEMOSTRACIÓN: Sean x, y, z los pies de las perpendiculares a r por a, b, c y sea m el punto medio $M(xmz)$. Sea $d = S_m a$. La primera parte del teorema anterior nos da que $d \sim_z c$. El teorema 3.69 nos da entonces que $b - R - d$ y la segunda parte del teorema anterior (aplicada ahora a las perpendiculares by y dz) implica que $b - R - c$. ∎



Ahora podemos probar una ligera variante del axioma **A7**:

Teorema 3.72 $a - p - c \wedge q - c - b \rightarrow \bigvee x(a - x - b \wedge q - p - x)$.

La figura muestra la situación de este teorema (a la izquierda) y la de **A7** (a la derecha):



DEMOSTRACIÓN: Supongamos en primer lugar $\mathrm{Col}(pqc)$ y distinguimos a su vez dos subcasos:

Si $q - p - c$, como $q - c - b$, también $q - p - b$, y basta tomar $x = b$.
Si $\neg q - p - c$, entonces $q \sim_p c$. Como $c - p - a$, tenemos que q está en la semirrecta opuesta a a respecto de p, luego $q - p - a$. Basta tomar $x = a$.

Pasamos ahora al caso en que $\neg\mathrm{Col}(pqc)$, de modo que $R = pq \neq cp$. Distinguimos también dos subcasos:

Si $a \in R$, entonces $a = p$, porque ambos están en $R \cap cp$. Basta tomar $x = a = p$.

Si $a \notin R$, puesto que $c - p - a$, tenemos que $c - R - a \wedge q \in R \wedge c \sim_q b$, luego el teorema anterior implica $b - R - a$. Por lo tanto existe un $x \in R$ tal que $b - x - a$. Ahora aplicamos **A7** al triángulo $\widehat{abc}$. El segmento $\overline{qx}$ debe cortar a $\overline{ac}$, luego existe un punto t tal que $q - t - x \wedge a - t - c$. Pero entonces $t, p \in ac \cap qx$, luego $p = t$. Esto implica que x cumple lo requerido. ■

3.7.2 La relación "estar al mismo lado de una recta"

Tras haber definido lo que es que una recta separe dos puntos podemos definir cuándo dos puntos están al mismo lado de una recta:

Definición 3.73 $a \sim_{pq} b \leftrightarrow p \neq q \wedge \bigvee c(a - pq - c \wedge b - pq - c)$.

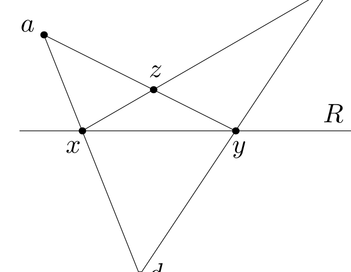
Se trata de una fórmula que depende de cuatro variables que representan puntos, pero como p y q sólo intervienen a través de la recta que definen, cuando no sea relevante destacar dos puntos de la recta escribiremos simplemente

$$a \sim_R b \leftrightarrow \bigvee c(a - R - c \wedge b - R - c).$$

En definitiva, dos puntos están al mismo lado de una recta si ésta los separa de un mismo punto c. En realidad, dicho punto c lo podemos fijar de antemano:

Teorema 3.74 $a - R - c \rightarrow (a \sim_R b \leftrightarrow b - R - c)$.

Demostración: Suponemos $a - R - c$. Entonces, si se cumple $b - R - c$, tenemos $a \sim_R b$ por definición.



Supongamos ahora $a \sim_R b$. Esto significa que existe un punto d tal que $a-R-d \wedge b-R-d$, y a su vez esto significa que existen puntos $x, y \in R$ tales que $a-x-d \wedge b-y-d$. Además las definiciones exigen que $a, b, c, d \notin R$.

Por **A7** aplicado al triángulo $\widehat{yxa}$, existe un z tal que $x-z-b \wedge y-z-a$. Podemos suponer que $z \notin R$, pues si $z \in R$ entonces z está tanto en $R \cap bx$ como en $R \cap ay$, luego $z = x = y$, luego $\mathrm{Col}(abx)$ y, más concretamente, $x - a - b \vee x - b - a$, pues $a \sim_R b$, y entonces basta tomar $z' = a$ o bien $z' = b$ para que se cumpla igualmente $x - z' - b \wedge y - z' - a$, pero ahora $z' \notin R$.

Así pues, tenemos que $a \sim_y z \wedge z \sim_x b \wedge a - R - c$. El teorema 3.71 implica que $z - R - c$ y, en una segunda aplicación, que $b - R - c$. ■

Ahora podemos probar algunos resultados básicos sobre esta relación:

Teorema 3.75 *Se cumple:*

1. $a - R - b \rightarrow \neg a \sim_R b$,
2. $a \notin R \rightarrow \bigvee c\ a - R - c$,
3. $a \notin R \rightarrow a \sim_R a$,
4. $a \sim_R b \rightarrow b \sim_R a$,
5. $a \sim_R b \wedge b \sim_R c \rightarrow a \sim_R c$.

Demostración: 1) Si $a \sim_R b$ el teorema anterior implica que $b - R - b$, lo cual es absurdo.

2) Basta tomar cualquier $t \in R$ y a su vez un c tal que $c - t - a$ con $c \neq a$.

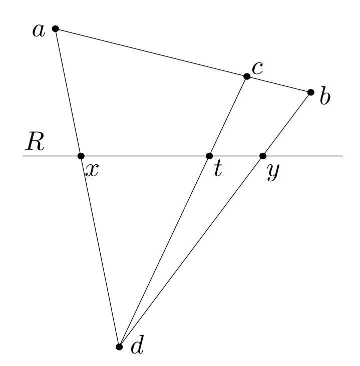
3) es consecuencia de 2).

4) es inmediata.

5) Si $a \sim_R b$ existe un d tal que $d - R - a \wedge d - R - b$ y, por el teorema anterior tenemos que $d - R - c$, luego $a \sim_R c$ por definición. ■

Veamos ahora un resultado de convexidad: si dos puntos están al mismo lado de una recta, todos los puntos intermedios cumplen lo mismo.

Teorema 3.76 $a \sim_R b \wedge a - c - b \rightarrow c \sim_R a$.



DEMOSTRACIÓN: Por definición de $\sim_R$ existe un punto d tal que $d - R - a \wedge d - R - b$, luego existen puntos $x, y \in R$ tales que $d - x - a \wedge d - y - b$. El teorema 3.7 nos da un punto t tal que $x - t - y \wedge d - t - c$. Consecuentemente, $c - R - d$ (aquí usamos que $c \notin R$, pues en otro caso $a - R - b$, y entonces $\neg a \sim_R b$). Así llegamos a que $c - R - d \wedge a - R - d$, luego $c \sim_R a$. ■

Ahora relacionamos las dos relaciones que hemos definido para rectas con sus análogas para puntos:

Teorema 3.77 *Se cumple:*

1. $p \in R \wedge \mathrm{Col}(abp) \rightarrow (a - R - b \leftrightarrow a - p - b \wedge a \notin R \wedge b \notin R)$,
2. $p \in R \wedge \mathrm{Col}(abp) \rightarrow (a \sim_R b \leftrightarrow a \sim_p b \wedge a \notin R)$.

DEMOSTRACIÓN: 1) Si $a - R - b$ existe un t tal que $a - t - b \wedge t \in R$, pero necesariamente $t = p$, pues ambos puntos están en $R \cap ab$. Por lo tanto $a \sim_p b$. La implicación opuesta es obvia.

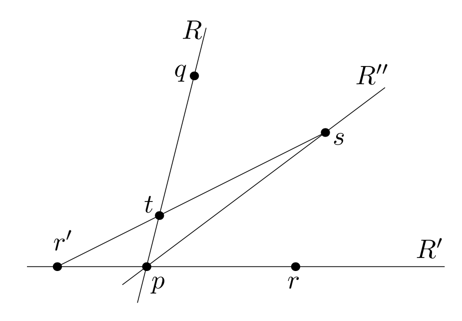
2) Sea c tal que $c - p - a$. Entonces, para todo $a \notin R$,

$$a \sim_R b \leftrightarrow c - R - b \leftrightarrow c - p - b \leftrightarrow a \sim_p b,$$

donde en la primera equivalencia hemos usado el teorema 3.74, en la segunda el apartado 1) de este teorema y en la tercera el teorema 3.32. ■

Terminamos con una propiedad técnica de separación que necesitaremos en diversas ocasiones:

Teorema 3.78 $s \sim_{pq} r \wedge s \sim_{pr} q \rightarrow q - sp - r$.



DEMOSTRACIÓN: Llamemos $R = pq$, $R' = pr$, $R'' = ps$ y sea $r' - p - r \wedge r' \neq p$. Entonces $r' - R - r \sim_R s$, luego existe un punto $t \in R$ tal que $r' - t - s$, luego $r \sim_{r'} s$, luego la segunda parte del teorema anterior nos da que $t \sim_{R''} q$.

Como $t \sim_s r' \wedge r' - R'' - r$, el teorema 3.71 nos da que $t - R'' - r$, y esto unido a $t \sim_{R''} q$ implica, por el teorema 3.74, que $q - R'' - r$. ■

3.7.3 Planos y semiplanos

Ya estamos en condiciones de definir el concepto de plano:

Definición 3.79 El *plano* que pasa por tres puntos a, b, c se define como

$$abc = \{x \mid x \sim_{ab} c \lor x \in ab \lor x - ab - c\}.$$

La definición sólo tiene interés en el caso en que $\neg\mathrm{Col}(abc)$. Teniendo en cuenta que a y b sólo intervienen en la definición a través de la recta ab, podemos no hacer referencia a dos puntos en concreto y considerar una recta R y un punto $r \notin R$, de modo que

$$P(R, r) = \{x \mid x \sim_R r \lor x \in R \lor x - R - r\}.$$

Con esta notación, $abc = P(ab, c)$. En otras palabras, el plano determinado por la recta R y el punto $r \notin R$ consta de los puntos de R, de los puntos que están al mismo lado que r respecto de R y de los puntos separados de r por R.

Podemos volver más simétrica esta definición a través del concepto de *semiplano:*

$$SP(p, q, r) = \{x \mid x \sim_{pq} r\}.$$

Como en el caso de los planos, la definición sólo depende de p y q a través de la recta pq, luego podemos definir

$$SP(R, r) = \{x \mid x \sim_R r\}$$

y así $SP(p, q, r) = SP(pq, r)$.

En estos términos, cada plano es la unión de una recta y los dos semiplanos complementarios que determina:

Teorema 3.80 $r' - R - r \to P(R, r) = SP(R, r) \cup R \cup SP(R, r')$.

Demostración: Si $x \in P(R, r)$ hay tres posibilidades:

Si $x \sim_R r$, entonces $x \in SP(R, r)$, por la definición de semiplano, luego está en la unión.

Si $x \in R$ obviamente está en la unión.

Si $x - R - r$, entonces $x \sim_R r'$ por el teorema 3.74, luego $x \in SP(R, r')$.

Esto nos da una inclusión, y la otra se prueba de forma similar. ■

Tenemos, pues, que un plano está determinado por tres puntos no colineales, pero de momento no podemos asegurar que los mismos puntos no puedan determinar planos distintos, pues no sabemos si $abc = bca$, por ejemplo. Para demostrar esta simetría, así como la unicidad del plano que pasa por tres puntos dados, necesitamos algunos resultados previos.

En primer lugar demostraremos que en $P(R, r)$ podemos cambiar r por cualquier otro punto del plano que no esté en la recta:

Teorema 3.81 $r \notin R \wedge s \notin R \wedge s \in P(R,r) \to P(R,r) = P(R,s)$.

DEMOSTRACIÓN: Distinguimos tres casos:

1) Si $s \sim_R r$, tomamos $r' - R - r$ y, por el teorema 3.76 tenemos que $r' - R - s$, luego

$$P(R,r) = SP(R,r) \cup R \cup SP(R,r') = SP(R,s) \cup R \cup SP(R,r') = P(R,s),$$

donde la igualdad $SP(R,r) = SP(R,s)$ se sigue inmediatamente de que $\sim_R$ es una relación de equivalencia.

Si $s - R - r$, entonces, aplicando dos veces el teorema anterior,

$$P(R,r) = SP(R,r) \cup R \cup SP(R,s) = P(R,s).$$ ■

Ahora vamos a probar que dos rectas secantes definen un plano. Para ello probamos lo siguiente:

Teorema 3.82 $R \cap R' = \{p\} \wedge r \neq p \wedge r \in R' \wedge r \notin R \to R' \subset P(R,r)$.

DEMOSTRACIÓN: Por el teorema 3.77, 2), $\overrightarrow{pr} \subset SP(R,r) \subset P(R,r)$. En efecto, si $b \in \overrightarrow{pr}$, entonces $b \sim_p r \wedge b \neq p$, luego $b \notin R$, luego $b \sim_R r$, luego $b \in SP(R,r)$.

Tomemos un punto $r' - p - r$, de modo que $R' = \overrightarrow{pr} \cup \{p\} \cup \overrightarrow{pr'}$. Claramente $r' - R - r$, luego $r' \in P(R,r)$ por definición. Por la inclusión que acabamos de probar, $\overrightarrow{pr'} \subset P(R,r') = P(R,r)$, donde la última igualdad nos la da el teorema anterior. Por lo tanto $R' \subset P(R,r)$. ■

Definición 3.83 Si R y R' son rectas que se cortan en un punto p, podemos definir $P(R,R') = P(R,r')$, para cualquier punto $r' \in R'$, $r' \neq p$, ya que el teorema anterior prueba que si r'' cumple lo mismo entonces $r'' \in P(R,r')$, y el teorema 3.81 implica que $P(R,r') = P(R,r'')$, luego la definición no depende de la elección de r'.

El teorema siguiente nos permitirá probar a continuación que la definición de plano es totalmente simétrica:

Teorema 3.84

$$R \cap R' = \{p\} \to R \subset P(R,R') \wedge R' \subset P(R,R') \wedge P(R,R') = P(R',R).$$

DEMOSTRACIÓN: $R \subset P(R,R')$ por la propia definición, mientras que el teorema anterior implica que $R' \subset P(R,R')$. Por la simetría de las hipótesis basta probar que $P(R,R') \subset P(R',R)$, pues intercambiando los papeles de las rectas obtenemos la inclusión opuesta.

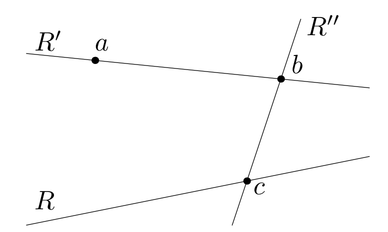
Pongamos que $P(R,R') = P(R,r')$, con $r' \in R'$, $r' \neq p$ y fijemos un punto tal que $r - p - r' \wedge r \neq p$.

Sea $s \in P(R, R') = P(R, r')$. Si $s \in R \vee s \in R'$, ya hemos visto que $s \in P(R', R)$, luego podemos suponer que $s \notin R \cup R'$. Entonces $s \in SP(R, r')$ o bien $s \in SP(R, r)$. Por simetría podemos suponer que $s \in SP(R, r')$, con lo que $s - R - r$. Esto significa que existe un $t \in R$ tal que $s - t - r$. Como $r \in R'$ y $r \neq p$, tiene que ser $r \neq t$. Por el teorema anterior $tr \subset P(R', t) = P(R', R)$, luego $s \in P(R', R)$. ■

En el teorema siguiente la variable P representa a un plano arbitrario, al igual que estamos usando R y R' para referirnos a rectas arbitrarias (técnicamente, para ajustarnos al lenguaje formal de la geometría de Tarski, en lugar de P deberíamos escribir uvw, para tres puntos bajo la hipótesis $\neg\mathrm{Col}(uvw)$).

Teorema 3.85 $a \in P \wedge b \in P \wedge a \neq b \rightarrow ab \subset P \wedge \bigvee c\ P = abc.$

DEMOSTRACIÓN: Sea $P = P(R, r)$ y sea $R' = ab$. Si $R = R'$ la conclusión es obvia, así que supondremos que $R \neq R'$. Entonces $a \notin R \vee b \notin R$. Suponemos sin pérdida de generalidad que $b \notin R$. Sea $c \in R \wedge c \notin R'$ y sea $R'' = cb$. Entonces



$$P = P(R, r) = P(R, b) = P(R, R'') =$$

$$P(R'', R) = P(R'', a) = P(R'', R') = P(R', R'') = P(R', c) = abc,$$

donde hemos usado, respectivamente, el teorema 3.81 (y que $b \notin R$), la definición de $P(R, R'')$, el teorema anterior, de nuevo el teorema 3.81, la definición de $P(R'', R)$, el teorema anterior, la definición de $P(R', R'')$ y la definición de $P(R', c)$. En particular $ab \subset P$. ■

Finalmente:

Teorema 3.86 $\neg\mathrm{Col}(abc) \wedge a \in P \wedge b \in P \wedge c \in P \rightarrow P = abc.$

DEMOSTRACIÓN: Por el teorema anterior existe un $r \notin ab$ tal que $P = abr$ luego, si llamamos $R = ab$, tenemos que $P = P(R, r) = P(R, c) = abc$, por el teorema 3.81. ■

Ahora ya son inmediatas las propiedades básicas de los planos. Usaremos la notación $P \in \mathcal{P}$ para indicar que P es un plano, es decir, que existen tres puntos no colineales tales que $P = abc$:

Teorema 3.87 *Se cumple:*

1. $\neg\mathrm{Col}(abc) \rightarrow \overset{1}{\bigvee} P \in \mathcal{P}(a \in P \wedge b \in P \wedge c \in P)$,
2. $\neg\mathrm{Col}(abc) \rightarrow abc = acb = bac = bca = cab = cba$,
3. $a \in P \wedge b \in P \wedge a \neq b \rightarrow ab \subset P$.

4. $R \subset P \cap P' \land P \neq P' \to R = P \cap P'$.

La última propiedad se debe a que si existiera $c \in P \cap P'$, $c \notin R$, entonces $P = P(R, c) = P'$.

Diremos que cuatro o más puntos son *coplanares* si están contenidos en un mismo plano. En particular

$$\mathrm{Cop}(abcd) \leftrightarrow \mathrm{Col}(abc) \lor (\neg\mathrm{Col}(abc) \land d \in abc)$$

Se cumple que cuatro puntos son coplanares si y sólo si están contenidos en dos rectas secantes:

Teorema 3.88 $\mathrm{Cop}(abcd) \leftrightarrow$

$$\bigvee x((\mathrm{Col}(abx) \land \mathrm{Col}(dcx)) \lor (\mathrm{Col}(acx) \land \mathrm{Col}(bdx)) \lor (\mathrm{Col}(adx) \land \mathrm{Col}(bdx))).$$

Demostración: Una implicación es obvia. Para demostrar la contraria suponemos que $a, b, c, d \in P$ y distinguimos varios casos:

Caso 1: Tres de los puntos son colineales, por ejemplo, $\mathrm{Col}(abc)$. Entonces basta tomar $x = c$, pues $\mathrm{Col}(abc) \land \mathrm{Col}(cdc)$.

Caso 2: Los puntos no son colineales tres a tres. Llamamos $R = ab$ y $R' = ac$, que son rectas distintas que se cortan en a. Además

$$P = abc = P(R, c) = P(R', b), \quad d \notin R, \quad d \notin R'.$$

Caso 2a: $c - R - d$. Entonces existe un punto $x \in R$ tal que $c - x - d$, y claramente cumple lo requerido.

Caso 2b: $b - R' - d$. Análogo.

Caso 2c: $d \sim_R c \land d \sim_{R'} b$, y el teorema 3.78 nos da que $b - ad - c$, es decir, que existe un $x \in ad$ tal que $b - x - c$, que también cumple lo requerido. ■

Capítulo IV

La geometría absoluta

En el capítulo anterior hemos mostrado que la geometría de Tarski permite hablar de puntos, rectas y planos, a pesar de que en principio sólo los puntos se encuentran entre sus conceptos primitivos. Ahora vamos a mostrar que en dicha axiomática es posible demostrar los resultados geométricos básicos sobre ángulos, triángulos, etc.

4.1 Simetrías axiales

En el capítulo anterior introdujimos ya el concepto de simetría puntual como auxiliar a la hora de definir las rectas y los planos, y para probar la existencia del punto medio de un segmento. Para los contenidos de este capítulo conviene introducir también el concepto de simetría axial.

Como ya tenemos probada la existencia del punto medio de un segmento, en lugar de $Mamb$, pasaremos a usar la notación Mab para referirnos al punto medio del segmento $\overline{ab}$.

El resultado básico sobre simetrías axiales es el siguiente:

Teorema 4.1 $\overset{1}{\bigvee} p'(Mpp' \in R \land (R \perp pp' \lor p = p'))$.

Es decir: dados un punto p y una recta R, existe otro punto p' que es el propio p si $p \in R$ y en caso contrario la recta pp'es perpendicular a R y la corta en el punto medio del segmento $\overline{pp'}$. El punto p' es el simétrico de p respecto de R.

Demostración: Si $p \notin R$, el teorema 3.63 nos da un único punto $x \in R$ (luego $x \neq p$) tal que $R \perp px$. Sea $p' = S_x p$, de modo que $Mpp' = x \in R$, y claramente $pp' = px$, luego $R \perp pp'$.

Además p' es único, pues si p'' cumple lo mismo, es decir, si

$$Mpp'' \in R \land (R \perp pp'' \lor p'' = p),$$

entonces tiene que ser $p'' \neq p$, ya que en caso contrario $p = Mpp'' \in R$, contradicción. Sea $x' = Mpp'' \in R$. Como $R \perp px'$, la unicidad hace que $x = x'$, luego $p' = S_x p = S_{x'} p = p''$.

En el caso en que $p \in R$, es obvio que $p' = p$ cumple lo pedido y, si p'' cumple también el enunciado, tiene que ser $p'' = p$, pues en caso contrario $x = Mpp'' \in R$, luego x y p son ambos el punto de corte de las rectas R y pp'' (que son distintas porque son perpendiculares), luego $x = p$ y $p = p''$, contradicción. ■

Definición 4.2 Definimos el *punto simétrico* de p respecto de la recta R como el único punto $S_R p$ que cumple el teorema anterior, es decir, el único punto p' tal que $Mpp' \in R \wedge (R \perp pp' \vee p = p')$.

Técnicamente, lo que hemos definido es una fórmula $p' = S_{ab} p$ con cuatro variables libres. Conviene adoptar el convenio de que S_{ab} representa la simetría axial determinada por la recta ab cuando $a \neq b$, mientras que representa la simetría puntual S_a si $a = b$.

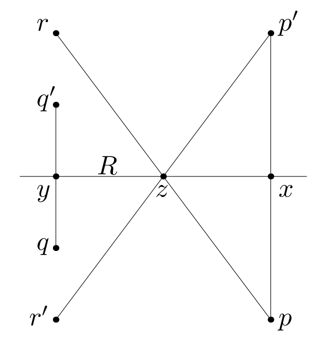
Las propiedades siguientes se demuestran sin dificultad:

Teorema 4.3 *Se cumple:*

1. $S_R p = p' \leftrightarrow S_S p' = p$,
2. $S_R S_R p = p$.
3. $\overset{1}{\bigvee} p' \; S_R p' = p$,
4. $S_R p = S_R q \leftrightarrow p = q$,
5. $S_R p = p \leftrightarrow p \in R$.

Al igual que las simetrías puntuales, las simetrías axiales son isometrías:

Teorema 4.4 $\overline{pq} \equiv \overline{S_R p \, S_R q}$.



Demostración: Sea $p' = S_R p$, $q' = S_R q$, $x = Mpp'$, $y = Mqq'$, $z = Mxy$, $r = S_z p$, $r' = S_z p'$.

Como $x = Mpp'$, aplicando S_z obtenemos que $y = Mrr'$, luego $r' = S_y r$. Aplicando S_y resulta que $\overline{qr} \equiv \overline{q'r'}$. Como $R \perp px \vee p = x$, se cumple $Rzxp$, luego, por definición de ángulo recto, $\overline{zp} \equiv \overline{zp'}$. Igualmente se demuestra que $\overline{zq} \equiv \overline{zq'}$. Es claro entonces que se cumple

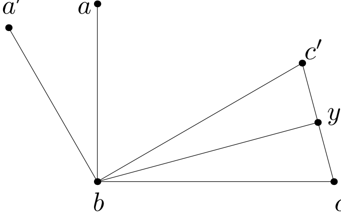
$$\mathrm{Ext}\begin{pmatrix} r & z & p & q \\ r' & z & p' & q' \end{pmatrix}.$$

Si $r \neq z$ el axioma **A5** nos da que $\overline{pq} \equiv \overline{p'q'}$, que es lo que había que probar, mientras que si $r = z$ llegamos a la misma conclusión porque $p = z = p'$ y sabemos que $\overline{zq} \equiv \overline{zq'}$. ■

Veamos un par de aplicaciones de las simetrías axiales. En primer lugar demostraremos que si dos triángulos rectángulos tienen los catetos iguales, entonces sus hipotenusas también son iguales:

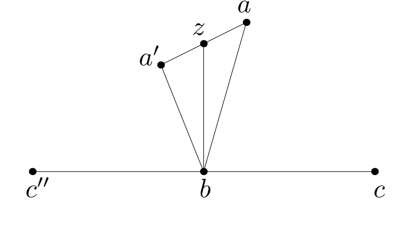
Teorema 4.5 $Rabc \wedge Ra'b'c' \wedge \overline{ab} \equiv \overline{a'b'} \wedge \overline{bc} \equiv \overline{b'c'} \rightarrow \overline{ac} \equiv \overline{a'c'}$.

DEMOSTRACIÓN: Sea $x = Mbb'$, sea $a_1 = S_x a'$, $c_1 = S_x c'$, y obviamente se cumple $b = S_x b'$. Como las simetrías son isometrías, tenemos que $(a', b', c') \equiv (a_1, b, c_1)$ y Ra_1bc_1. Por lo tanto, basta probar que $\overline{ac} \equiv \overline{a_1c_1}$ o, equivalentemente, podemos suponer que $b = b'$.



Bajo esta hipótesis, sea $y = Mcc'$, de modo que $Rbyc$, ya que $\overline{bc} \equiv \overline{bc'}$. Se cumple entonces que $C = S_{by}c'$, tanto si $b \neq y$ (por la propia definición de simetría axial) como si $b = y$, en cuyo caso se cumple por la definición de punto medio.

Sea $a'' = S_{by}a'$. De este modo, aplicando S_{by} obtenemos las congruencias $(a', b, c') \equiv (a'', b, c)$ y $Ra''bc$, luego basta probar que $\overline{ac} \equiv \overline{a''c}$. Equivalentemente, podemos suponer que $c = c'$.



Sea $z = Maa'$, de modo que $Rbza$, pues $\overline{ba} \equiv \overline{ba'}$. Esto implica que $a = S_{bz}a'$, y obviamente $b = S_{bz}b$. Sea $c'' = S_b c$.

Puesto que $Rabc$ y $Ra'bc$, tenemos que $\overline{ac} \equiv \overline{ac''}$ y $\overline{a'c} \equiv \overline{a'c''}$. Además $\mathrm{Col}(a, z, a')$, luego el teorema 3.19 (o trivialmente en el caso en que $a = a'$) implica que $\overline{zc} \equiv \overline{zc''}$, luego $Rzbc$, luego $c'' = S_{bz}c$.

Finalmente, aplicando S_{bz} a $\overline{ac} \equiv \overline{ac''}$ obtenemos $\overline{a'c} \equiv \overline{ac''} \equiv \overline{ac}$, como había que probar. ■

Para la segunda aplicación necesitamos una ligera variante del teorema 3.65:

Teorema 4.6 $a \in R \wedge q \notin R \rightarrow \bigvee p(R \perp pa \wedge p \sim_R q)$.

DEMOSTRACIÓN: Por el teorema 3.65 existe p' tal que $R \perp p'a$ y $q - R - p'$. Basta tomar $p = S_R p'$. Claramente $p - R - p'$, luego $p \sim_R q$, y $pa = p'a$. ■

Ahora ya podemos probar el resultado más general sobre transporte de triángulos: dado cualquier triángulo $\widehat{abc}$, podemos construir un único triángulo $\widehat{a'b'c'}$ congruente con el dado cuyo vértice c' esté en cualquier semiplano prefijado respecto de la recta $a'b'$.

Teorema 4.7

$$\neg\mathrm{Col}(a, b, c) \wedge \neg\mathrm{Col}(a', b', p) \wedge \overline{ab} \equiv \overline{a'b'} \rightarrow \overset{1}{\bigvee} c((a, b, c) \equiv (a', b', c) \wedge c' \sim_{a'b'} p).$$

DEMOSTRACIÓN: Veamos en primer lugar la existencia. Sea x el pie de la perpendicular a ab por c, es decir, el punto que cumple $cx \perp ab$ y $\mathrm{Col}(abx)$. Por el teorema 3.17 existe un x' tal que $(a, b, c) \equiv (a', b', x')$. Llamemos $R = a'b'$.

Sea q según el teorema anterior, es decir, $R \perp qx' \wedge q \sim_R p$. Por 3.35 existe un c' tal que $c' \sim_{x'} q \wedge \overline{x'c'} \equiv \overline{cx}$. Entonces, por el teorema 3.77, 2), se cumple que $c' \sim_R q$, luego $c' \sim_R p$.

Tenemos $Raxc \wedge Ra'x'c' \wedge Rbxc \wedge Rb'x'c'$, luego el teorema 4.5 implica que $\overline{ac} \equiv \overline{a'c'} \wedge \overline{bc} \equiv \overline{b'c'}$, luego $(a,b,c) \equiv (a',b',c')$ y c' cumple todo lo requerido.

Finalmente probamos la unicidad:

Si otro punto c'' cumple las mismas condiciones del enunciado, entonces $(a',b',c') \equiv (a',b',c'')$ y $c' \sim_R c''$. Sea $c^* = S_R c$. Claramente $c'' - R - c^*$, luego $c' - R - c^*$, luego existe un $t \in R$ tal que $c' - t - c^*$. Aplicando S_R obtenemos que $(a',b',c^*) \equiv (a',b',c'') \equiv (a',b',c')$. En particular $\overline{a'c'} \equiv \overline{a'c^*} \wedge \overline{b'c'} \equiv \overline{b'c^*}$. El teorema 3.19 nos da que $\overline{tc'} \equiv \overline{tc^*}$, luego $t = Mcc^*$. Entonces, como $\overline{a'c'} \equiv \overline{a'c^*}$, por definición $Ra'tc'$, e igualmente $Rb'tc'$. Esto implica que $R \perp cc^*$, luego $c^* = S_R c' = S_R c''$, luego $c' = c''$. ■

De aquí deducimos un resultado que necesitaremos después:

Teorema 4.8 $(a,b,c) \equiv (a',b',c') \wedge \mathrm{Col}(acd) \rightarrow \bigvee d'((a,b,c,d) \equiv (a',b',c',d'))$.

La última congruencia significa que cualquier par de puntos de la primera cuádrupla es congruente con el par correspondiente de la segunda.

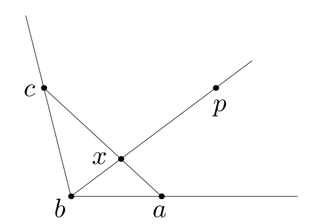
DEMOSTRACIÓN: Si $a \neq c$ el teorema 3.17 nos da un punto d' de manera que $(a,c,d) \equiv (a',c',d')$, y entonces se cumple Conf5 $\begin{pmatrix} a & c & d & b \\ a' & c' & d' & b' \end{pmatrix}$, luego $\overline{bc} \equiv \overline{b'd'}$, luego $(a,b,c,d) \equiv (a',b',c',d')$.

Si $a = c$, entonces $a' = c'$, y la existencia de d' la proporciona el teorema 3.17 o el teorema anterior según si a,b,d son colineales o no. ■

4.2 Ángulos

Definición 4.9 Llamaremos *ángulo* definido por tres puntos a,b,c al lugar geométrico

$$\widehat{abc} = \{p \mid a \neq b \neq c \wedge p \neq b \wedge \bigvee x(a - x - c \wedge (x = b \vee x \sim_b p))\}.$$



Si a,b,c no son colineales no puede suceder $x = b$ y el ángulo $\widehat{abc}$ es la unión de todas las semirrectas de origen b que pasan por un punto x del segmento $\overline{ac}$. Esto incluye a las semirrectas $\overrightarrow{ba}$ y $\overrightarrow{bc}$, que se llaman *lados* del ángulo. Notemos que, con la definición que hemos dado, el punto b (el *vértice* del ángulo) no pertenece al ángulo.

Si a, b, c son colineales, hay dos posibilidades: si $a \sim_b c$, entonces tampoco puede suceder $x = b$ y se cumple que $\widehat{abc} = \overrightarrow{ba} = \overrightarrow{bc}$. Diremos que el ángulo es *nulo*.

Si $a - b - c$ entonces tomando $x = b$ se cumple que todo punto $p \neq b$ está en $\widehat{abc}$. En este caso diremos que el ángulo es *llano*. En realidad, para ajustarnos a las definiciones tradicionales, los ángulos llanos, como lugares geométricos, deberían ser los semiplanos, pero este convenio que estamos adoptando nos resultará más cómodo en la práctica.

Claramente $\widehat{abc} = \widehat{cba}$. Veamos ahora que si cambiamos a y b por puntos que determinen la misma semirrecta de origen b, el ángulo definido sigue siendo el mismo. Un poco más en general:

Teorema 4.10 $p \in \widehat{abc} \wedge a' \sim_b a \wedge c' \sim_b c \wedge p' \sim_b p \rightarrow p' \in \widehat{a'bc'}$.

DEMOSTRACIÓN: Si $a - b - c$, también $a' - b - c'$, y la conclusión es trivial, pues la cumplen todos los puntos $p' \neq b$. Podemos suponer, pues, que el ángulo no es llano, por lo que existe un x tal que $a - x - c \wedge x \sim_b p$.

Aplicando el axioma **A7** o el teorema 3.72 según si $b - a - a'$ o $b - a' - a$, obtenemos un punto x' tal que $a' - x' - c \wedge x \sim_b x'$, luego $x' \sim_b p \sim_b p'$. Concluimos que $p' \in \widehat{a'b'c}$ y el mismo argumento nos permite concluir que $p' \in \widehat{a'b'c'}$. ■

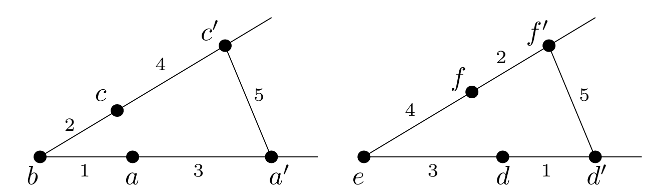
4.2.1 Congruencia de ángulos

Introducimos ahora el concepto de congruencia de ángulos, cuya interpretación es la obvia: dos ángulos son congruentes si uno puede trasladarse hasta superponerse al otro. En la definición introducimos un pequeño artificio que la simplifica, pero enseguida veremos dos caracterizaciones totalmente naturales.

Definición 4.11 Diremos que dos ángulos son *congruentes* si cumplen:

$$\widehat{abc} \equiv \widehat{def} \leftrightarrow a \neq b \neq c \wedge d \neq e \neq f \wedge$$

$$\bigvee a'c'd'f'(b - a - a' \wedge b - c - c' \wedge e - d - d' \wedge e - f - f' \wedge$$
$$\overline{aa'} \equiv \overline{ed} \wedge \overline{bc'} \equiv \overline{ef} \wedge \overline{dd'} \equiv \overline{ba} \wedge \overline{ff'} \equiv \overline{bc} \wedge \overline{a'c'} \equiv \overline{d'f'}).$$



El teorema siguiente expresa más claramente la idea:

Teorema 4.12 *Las afirmaciones siguientes son equivalentes:*

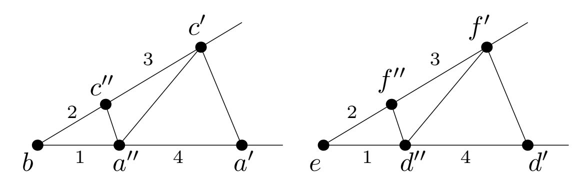
1. $\widehat{abc} \equiv \widehat{def}$,
2. $\bigvee a'c'd'f'(a' \sim_b a \wedge c' \sim_b c \wedge d' \sim_e d \wedge f' \sim_e f \wedge (a', b, c') \equiv (d', e, f'))$,
3. $a \neq b \neq c \wedge d \neq e \neq f \wedge$
   $\bigwedge a'c'd'f'(a' \sim_b a \wedge c' \sim_b c \wedge d' \sim_e d \wedge f' \sim_e f \wedge$
   $\overline{ba'} \equiv \overline{ed'} \wedge \overline{bc'} \equiv \overline{ef'} \rightarrow \overline{a'c'} \equiv \overline{d'f'})$.

En definitiva, dos ángulos son congruentes si cuando fijamos puntos a', c' en los lados de uno y d', f' en los lados del otro de modo que $\overline{ba'} \equiv \overline{ed'} \wedge \overline{bc'} \equiv \overline{ef'}$, también se cumple que $\overline{a'c'} \equiv \overline{d'f'}$.

Demostración: 1) $\Rightarrow$ 2) Sean a', c', d', f' puntos según la definición de congruencia de ángulos. Claramente $a' \sim_b a \wedge c' \sim_b c \wedge d' \sim_e d \wedge f' \sim_e f$. Como $\overline{aa'} \equiv \overline{ed} \wedge \overline{dd'} \equiv \overline{ba}$, el teorema 3.3 implica que $\overline{ba'} \equiv \overline{ed'}$, e igualmente $\overline{bc'} \equiv \overline{ef'}$, luego $(a', b, c') \equiv (d', e, f')$ y se cumple 2).

2) $\Rightarrow$ 3) Fijemos a', c', d', f' según las hipótesis de 2), que en particular implican que $a \neq b \neq c \wedge d \neq e \neq f$ por definición de $\sim$. Ahora tomemos a'', c'', d'', f'' en las condiciones de 3), de modo que tenemos que demostrar que $\overline{a''c''} \equiv \overline{d''f''}$.

En definitiva tenemos, como muestra la figura, cuatro pares de puntos en los lados de los ángulos, de modo que cada uno dista del vértice de su ángulo lo mismo que su pareja del suyo. El teorema 3.11 implica además las congruencias $\overline{a'a''} \equiv \overline{d'd''} \wedge \overline{c'c''} \equiv \overline{f'f''}$, que también se indican en la figura:



En particular $(b, a', a'') \equiv (e, d', d'')$, luego

$$\text{Conf5}\begin{pmatrix} b & a' & a'' & c' \\ e & d' & d'' & f' \end{pmatrix}$$

(y $b \neq a'$), luego $\overline{c'a''} \equiv \overline{f'd''}$. Esto a su vez implica

$$\text{Conf5}\begin{pmatrix} b & c' & c'' & a' \\ e & f' & f'' & d'' \end{pmatrix},$$

lo que nos da $\overline{a''c''} \equiv \overline{d''f''}$, que es lo que había que probar.

3) $\Rightarrow$ 1) Dados $\widehat{abc}$ y $\widehat{def}$, el teorema 3.35 nos permite construir puntos a', c', d', f' que cumplen las condiciones de la definición de congruencia de ángulos salvo quizá la última, pero ésta la proporciona 3). ■

Ahora es fácil demostrar las propiedades elementales de la congruencia:

Teorema 4.13 *Se cumple:*

1. $a \neq b \neq c \to \widehat{abc} \equiv \widehat{abc}$,

2. $\widehat{abc} \equiv \widehat{def} \to \widehat{def} \equiv \widehat{abc}$,

3. $\widehat{abc} \equiv \widehat{def} \land \widehat{def} \equiv \widehat{ghi} \to \widehat{abc} \equiv \widehat{ghi}$,

4. $a \neq b \neq c \to \widehat{abc} \equiv \widehat{cba}$.

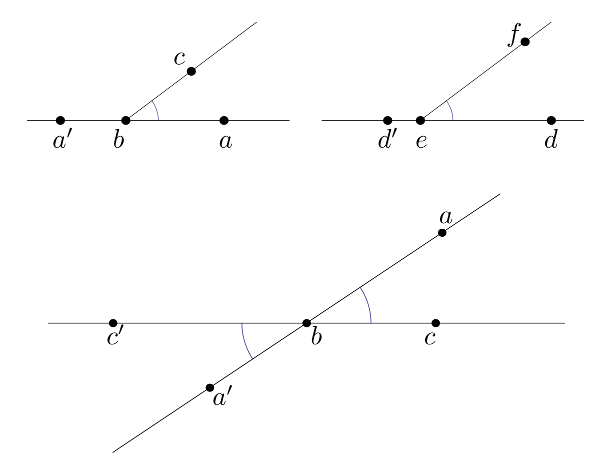
Podríamos probar que $\widehat{abc} = \widehat{a'b'c'} \to \widehat{abc} \equiv \widehat{a'b'c'}$, lo cual no es trivial, pues exige demostrar que un ángulo determina su vértice y sus lados, pero no vamos a necesitar este hecho.

Los suplementarios de ángulos congruentes son congruentes, y dos ángulos opuestos por el vértice son congruentes:

Teorema 4.14 *Se cumple:*

1. $\widehat{abc} \equiv \widehat{def} \land a - b - a' \land a' \neq b \land d - e - d' \land d' \neq e \to \widehat{a'bc} \equiv \widehat{d'ef}$,

2. $a - b - a' \land a \neq b \neq a' \land c - b - c' \land c \neq b \neq c' \to \widehat{abc} \equiv \widehat{a'bc'}$.



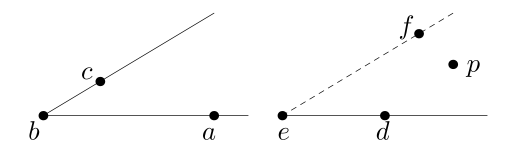
DEMOSTRACIÓN: 1) El teorema 3.35 nos da puntos d_0, f_0, d_0' que verifican $d_0 \sim_e d \land f_0 \sim_e f \land d_0' \sim_e d'$ y $\overline{ed_0} \equiv \overline{ba} \land \overline{ef_0} \equiv \overline{bc} \land \overline{ed_0'} \equiv \overline{ba'}$. El teorema 4.12 implica entonces que $\overline{ac} \equiv \overline{d_0 f_0}$. El axioma **A5** implica que $\overline{a'c} \equiv \overline{d_0' f_0}$ y el teorema 4.12 nos permite concluir que $\widehat{a'bc} \equiv \widehat{d'ef}$.

2) es consecuencia inmediata de 1), pues dos ángulos opuestos por el vértice son suplementarios del mismo ángulo. ■

Ahora probamos un resultado fundamental sobre congruencia de ángulos, y es que los ángulos pueden trasladarse, de forma única si se especifican condiciones adecuadas:

Teorema 4.15 $\neg\mathrm{Col}(abc) \land \neg\mathrm{Col}(dep) \to \bigvee f(\widehat{abc} \equiv \widehat{def} \land f \sim_{ed} p) \land$

$$\bigwedge f_1 f_2(\widehat{abc} \equiv \widehat{def_1} \land \widehat{abc} \equiv \widehat{def_2} \land f_1 \sim_{ed} p \land f_2 \sim_{ed} p \to f_1 \sim_e f_2).$$



Los datos son un ángulo $\widehat{abc}$, una semirrecta $\overrightarrow{ed}$ y un punto p que determina un semiplano de la recta ed, y lo que probamos es que existe una única semirrecta $\overrightarrow{ef}$ contenida en el semiplano determinado por p tal que el ángulo $\widehat{edf}$ es congruente con el dado.

Notemos que la unicidad de la semirrecta no significa la unicidad de f, sino que si dos puntos cumplen lo exigido a f, entonces ambos determinan la misma semirrecta de origen d.

DEMOSTRACIÓN: Por el teorema 3.35 existe un punto d' tal que $d' \sim_e d$ y $\overline{ed'} \equiv \overline{bc}$. Por 4.7 existe un único punto f tal que $f \sim_{ed} p$ y $(a,b,c) \equiv (d',e,f)$, lo que en particular implica que $\widehat{abd} \equiv \widehat{def}$.

Para probar la unicidad suponemos que existe otro punto f_1 que cumple $\widehat{abc} \equiv \widehat{def_1} \land f_1 \sim_{ed} p$. Tomamos entonces f' tal que $f' \sim_e f_1$ y $\overline{ef'} \equiv \overline{ef}$. La congruencia de ángulos implica que $\overline{fd} \equiv \overline{f'd'}$ y por consiguiente tenemos que $(a,b,c) \equiv (d',e,f) \equiv (d',e,f')$. La unicidad de f implica a su vez que $f' = f$, luego $f_1 \sim_e f$. ■

Ahora probamos que todos los ángulos rectos son congruentes, que todo ángulo congruente con un ángulo recto es recto y que un ángulo es recto si y sólo si es congruente con su suplementario:

Teorema 4.16 *Se cumple:*

1. $Rabc \land a \neq b \neq c \land Ra'b'c' \land a' \neq b' \neq c' \to \widehat{abc} \equiv \widehat{a'b'c'}$,
2. $Rabc \land \widehat{abc} \equiv \widehat{a'b'c'} \to Ra'b'c'$,
3. $c - b - d \land c \neq b \neq d \land a \neq b \to (Rabc \leftrightarrow \widehat{abc} \equiv \widehat{abd})$.

DEMOSTRACIÓN: 1) Podemos tomar a'' y b'' tales que $a' \sim_{b'} a''$, $c' \sim_{b'} c''$, $\overline{a''b'} \equiv \overline{ab}$, $\overline{c''b'} \equiv \overline{cb}$. Entonces $Rabc \land Ra''b'c''$ y son dos triángulos rectángulos con catetos iguales, luego el teorema 4.5 implica que $\overline{ac} \equiv \overline{a''c''}$, lo que a su vez implica que $\widehat{abc} \equiv \widehat{a'b'c'}$.

2) Tomamos a'' y c'' igual que antes. Ahora es la congruencia de los ángulos la que nos da que $\overline{ac} \equiv \overline{a''c''}$, luego $(a,b,c) \equiv (a'',b',c'')$, luego el teorema 3.60 implica que $Ra''b'c''$, y por 3.58, 5) también $Ra'b'c'$.

3) Si $c' = S_b c$, ambos miembros de la coimplicación equivalen a $\overline{ac'} \equiv \overline{ac}$. ■

Ahora ya podemos dar condiciones que garanticen la unicidad de la perpendicular a una recta por uno de sus puntos. Como es habitual, en el teorema siguiente P representa un plano:

Teorema 4.17 $x \in R \wedge R \subset P \rightarrow \overset{1}{\bigvee} S(S \perp R \wedge x \in S \wedge S \subset P)$.

DEMOSTRACIÓN: Sea $c \in P \setminus R$. Por el teorema 3.65 existen puntos p, t tales que $px \perp R \wedge t \in R \wedge c - t - p$. Como $c, t \in P$, se cumple que $ct \subset P$, luego $p \in P$, luego $S = px \subset P$, y obviamente $S \perp R$.

Si $S' = xp'$ cumple lo mismo, podemos suponer que $p' \sim_R p$ y, fijado un punto $y \in R$, $y \neq x$, tenemos que $Ryxp \wedge Ryxp'$, luego el teorema anterior nos da la congruencia $\widehat{yxp} \equiv \widehat{yxp'}$. El teorema 4.15 nos da que $p \sim_x p'$, luego $S = S'$. ■

Dejamos al lector la prueba de que todos los ángulos nulos son congruentes entre sí, al igual que todos los ángulos llanos:

Teorema 4.18 *Se cumple:*

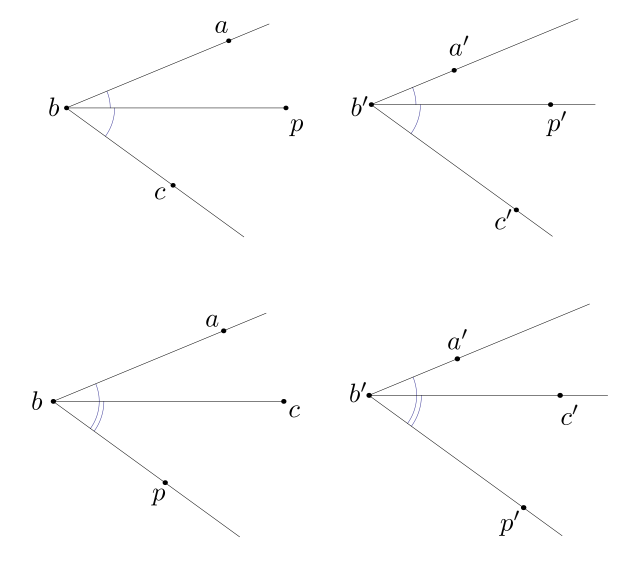
1. $a \sim_b c \rightarrow (\widehat{abc} \equiv \widehat{a'b'c'} \leftrightarrow a' \sim_{b'} c')$,
2. $a - b - c \wedge a \neq b \neq c \rightarrow (\widehat{abc} \equiv \widehat{a'b'c'} \leftrightarrow a' - b' - c' \wedge a' \neq b' \neq c')$.

(Para la segunda parte se usa el teorema 3.13.)

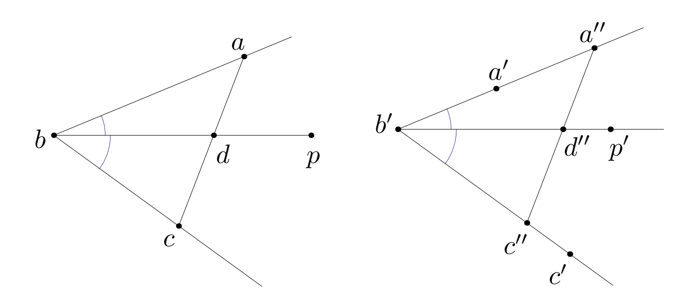
Para terminar demostramos que es posible sumar y restar ángulos:

Teorema 4.19 $((a - bp - c \wedge a' - b'p' - c') \vee (a \sim_{bp} c \wedge a' \sim_{b'p'} c')) \wedge$

$$\widehat{abp} \equiv \widehat{a'b'p'} \wedge \widehat{pbc} \equiv \widehat{p'b'c'} \rightarrow \widehat{abc} \equiv \widehat{a'b'c'}.$$



Demostración: Distingamos los dos casos que aparecen en la hipótesis. Supongamos en primer lugar que $a - bp - c \wedge a' - b'p' - c'$. Por definición de separación de puntos por rectas existe un punto d tal que $a - d - c \wedge \mathrm{Col}(bpd)$



Observemos que en la figura el punto d cumple $d \sim_p b$, pero esto no es necesariamente cierto en general. Puede ocurrir $d = b$ si el ángulo $\widehat{abc}$ es llano, o también $d - b - p$.

Sea a'' tal que $a'' \sim_{b'} a' \wedge \overline{b'a''} \equiv \overline{ba}$. Si $d \neq p$ el teorema 3.35 nos da un punto d'' tal que $\mathrm{Col}(b'p'd'') \wedge (d'' \sim_{b'} p' \leftrightarrow d \sim_p b) \wedge \overline{b'd''} \equiv \overline{bd}$, es decir, tomamos d'' al mismo lado que p' respecto de b' o en el lado opuesto según la relación de d respecto de p. Si $d = p$ esto se cumple también tomando $d'' = b'$.

A su vez tomamos un punto c'' tal que $a'' - d'' - c'' \wedge \overline{d''c''} \equiv \overline{dc}$.

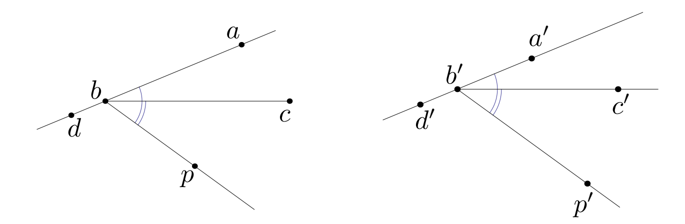
Si $d \neq b$ entonces $\widehat{abp} \equiv \widehat{a'b'p'}$ implica que $\overline{ad} \equiv \overline{a''d''}$, y lo mismo vale trivialmente si $d = b$, pues entonces $b' = d''$ y la congruencia se reduce a $\overline{ab} \equiv \overline{a''b'}$. Por lo tanto tenemos $\mathrm{Ext}\begin{pmatrix} a & d & c & b \\ a'' & d'' & c'' & b' \end{pmatrix}$, luego $\overline{bc} \equiv \overline{b'c''}$.

Ahora tenemos que $(c, b, d) \equiv (c'', b', d'')$, luego si $b \neq d$ concluimos que $\widehat{cbd} \equiv \widehat{c''b'd''}$, y esto implica que $\widehat{pbc} \equiv \widehat{p'b'c'}$, porque estos ángulos son iguales a los anteriores o bien son sus suplementarios (y entonces usamos 4.14), según que d esté al mismo lado que p respecto de b o en el lado opuesto. Si $b = d$ llegamos a la misma conclusión porque $\widehat{pbc}$ es suplementario de $\widehat{pba}$ y $\widehat{p'b'c''}$ es suplementario de $\widehat{p'b'a'}$.

Por otro lado tenemos que $\widehat{pbc} \equiv \widehat{p'b'c'}$, y c', c'' están ambos separados de a por $b'p'$, luego $c' \sim_{p'b'} c''$. El teorema 4.15 implica que $c' \sim_{b'} c''$.

Por último tenemos que $(a, b, c) \equiv (a'', b', c'')$, luego $\widehat{abc} \equiv \widehat{a''b'c''} \equiv \widehat{a'b'c'}$.

Ahora suponemos el segundo caso, es decir, que $a \sim_{bp} c \wedge a' \sim_{b'c'} c'$.



Entonces tomamos puntos $d - b - a \wedge d \neq b$, $d' - b' - a' \wedge d' \neq b'$. Así, puesto que $\widehat{abp} \equiv \widehat{a'b'p'}$, también $\widehat{dbp} \equiv \widehat{d'b'p'}$ (porque son ángulos suplementarios de los anteriores), pero ahora $d - bp - c \wedge d' - b'p' - c'$, por lo que el caso ya probado nos permite concluir que $\widehat{dbc} \equiv \widehat{d'b'c'}$. Pasando de nuevo a los ángulos suplementarios obtenemos $\widehat{abc} \equiv \widehat{a'b'c'}$. ■

4.2.2 Ordenación de ángulos

Seguidamente definimos la relación de orden natural entre ángulos:

Definición 4.20 $\widehat{abc} \leq \widehat{def} \leftrightarrow a \neq b \neq c \wedge d \neq e \neq f \wedge \bigvee p(p \in \widehat{def} \wedge \widehat{abc} \equiv \widehat{dep})$.

Probamos en primer lugar que esta relación se cumple trivialmente en el caso de ángulos nulos y llanos, en el sentido de que todo ángulo nulo es menor o igual que cualquier otro y todo ángulo llano es mayor o igual que cualquier otro:

Teorema 4.21 *Se cumple:*

1. $a \sim_b c \wedge d \neq e \neq f \rightarrow \widehat{abc} \leq \widehat{def}$,
2. $a \neq b \neq c \wedge d - e - f \rightarrow \widehat{abc} \leq \widehat{def}$.

Demostración: 1) Trivialmente $d \in \widehat{def}$ y $\widehat{ded} \equiv \widehat{abc}$, porque todos los ángulos nulos son congruentes (teorema 4.18). Esto prueba la desigualdad.

2) Por 1) podemos suponer que $\widehat{abc}$ no es nulo. Por el teorema 4.15 (o trivialmente si el ángulo $\widehat{abc}$ es llano) existe $p \neq e$ tal que $\widehat{abc} \equiv \widehat{dep}$, y trivialmente $p \in \widehat{def}$, luego $\widehat{abc} \leq \widehat{def}$. ■

Veamos una caracterización de la relación de orden:

Teorema 4.22 $\widehat{abc} \leq \widehat{def} \leftrightarrow \bigvee q(c \in \widehat{abq} \wedge \widehat{abq} \equiv \widehat{def})$.

Demostración: Supongamos que $\widehat{abc} \leq \widehat{def}$, con lo que existe un $p \in \widehat{def}$ tal que $\widehat{abc} \equiv \widehat{dep}$.

Si $\widehat{def}$ es llano el resultado es trivial, pues basta tomar $q = S_b a$ (y trivialmente $c \in \widehat{abq}$). En caso contrario existe $x \sim_e p$ tal que $d - x - f$. Tomamos un

punto $a' \sim_b a \land \overline{ba'} \equiv \overline{ed}$ y $c' \sim_b c \land \overline{bc'} \equiv \overline{ex}$. La congruencia $\widehat{abc} \equiv \widehat{dep}$ implica que $\overline{c'd'} \equiv \overline{xd}$, luego $(a', b, c') \equiv (d, e, x)$. El teorema 4.8 nos da un punto q tal que $(a', b, c', q) \equiv (d, e, x, f)$, luego $a' - c' - q$ (por el teorema 3.13) y $\widehat{abq} \equiv \widehat{def}$. Como $c' \sim_b c$, concluimos que $c \in \widehat{abq}$.

Veamos ahora el recíproco:

Si $\widehat{def}$ es llano, la conclusión es trivial por el teorema anterior. Supongamos que no lo es, con lo que tampoco puede serlo $\widehat{abq}$, luego existe $x \sim_b c$ tal que $q - x - a$.

Tomamos $d' \sim_e f \land \overline{ed'} \equiv \overline{ba}$ y $f' \sim_e f \land \overline{ef'} \equiv \overline{bq}$. De este modo, la congruencia $\widehat{abq} \equiv \widehat{def}$ implica que $\overline{qa} \equiv \overline{f'd'}$, luego $(a, b, q) \equiv (d', e, f')$. Por el teorema 4.8 existe un punto p tal que $(a, b, q, x) \equiv (d', e, f', p)$. En particular $f' - p - d'$, luego $p \in \widehat{def}$ y $\widehat{dep} \equiv \widehat{abc}$, luego $\widehat{abc} \leq \widehat{def}$. ■

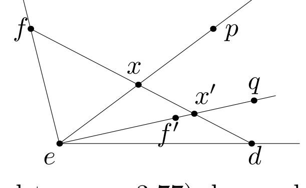
Ahora ya podemos probar las propiedades básicas de la relación de orden:

Teorema 4.23 *Se cumple:*

1. $\widehat{abc} \leq \widehat{def} \land \widehat{abc} \equiv \widehat{a'b'c'} \land \widehat{def} \equiv \widehat{d'e'f'} \to \widehat{a'b'c'} \leq \widehat{d'e'f'}$,
2. $a \neq b \neq c \to \widehat{abc} \leq \widehat{abc}$,
3. $\widehat{abc} \leq \widehat{def} \land \widehat{def} \leq \widehat{abc} \to \widehat{abc} \equiv \widehat{def}$,
4. $\widehat{abc} \leq \widehat{def} \land \widehat{def} \leq \widehat{ghi} \to \widehat{abc} \leq \widehat{ghi}$,
5. $a \neq b \neq c \land d \neq e \neq f \to \widehat{abc} \leq \widehat{def} \lor \widehat{def} \leq \widehat{abc}$.

Demostración: Probaremos por ejemplo la 3) y la 5).

3) Si los dos ángulos son llanos sabemos que son congruentes, luego podemos suponer que al menos uno de ellos no lo es. No perdemos generalidad si suponemos concretamente que $\widehat{def}$ no es llano.



Sea $p \in \widehat{def}$ tal que $\widehat{ped} \equiv \widehat{abc}$. Sea $x \sim_e p$ tal que $f - x - d$. Entonces $\widehat{def} \leq \widehat{abd} \equiv \widehat{ped} \equiv \widehat{xed}$, luego existe un $q \in \widehat{xed}$ tal que $\widehat{def} \equiv \widehat{deq}$. Notemos que no puede ser $x - e - d$, pues entonces $f - e - d$ y $\widehat{dfe}$ sería llano. Sea $x' \sim_e q$ tal que $x - x' - d$. Así $\widehat{dex'} \equiv \widehat{deq} \equiv \widehat{def}$. Sea $f' \sim_e x'$ tal que $\overline{ef'} \equiv \overline{ef}$. Entonces $(e, d, f) \equiv (e, d, f')$ y $f' \sim_{ed} x' \sim_{ed} f$ (por el teorema 3.77), luego el teorema 4.7 implica que $f = f'$, de donde $f = x'$ (ambos son el punto de corte de $eq = ef$ y fd) y $x = x'$, luego $\overrightarrow{ep} = \overrightarrow{ef}$, luego $\widehat{abc} \equiv \widehat{dep} \equiv \widehat{def}$.

5) Podemos suponer que los ángulos no son ni nulos ni llanos, pues en tal caso la conclusión es obvia. Por el teorema 4.15 existe un punto c' tal que $c' \sim_{ba} c \land \widehat{def} \equiv \widehat{abc'}$. En particular $p \in abc$, luego, por la definición de plano, tenemos tres posibilidades:

1. $c' \in bc$, en cuyo caso $\widehat{abc} \equiv \widehat{abc'} \equiv \widehat{def}$.

2. $c' - bc - a$, en cuyo caso existe un punto $x \in bc$ tal que $c' - x - a$. En particular $c' \sim_a c$, luego $c' \sim_{ab} x$ por 3.77, luego $c \sim_{ab} x$, luego $c \sim_b x$ por el mismo teorema, y así podemos concluir que $c \in \widehat{abc'}$. Esto a su vez implica que $\widehat{abc} \leq \widehat{abc'} \equiv \widehat{def}$.

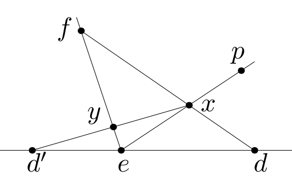
3. $c' \sim_{bc} a$, en cuyo caso, como también $c' \sim_{ab} c$, el teorema 3.78 nos da que $c - bc' - a$, y concluimos como en el caso anterior intercambiando los papeles de c y c'. ■

Para terminar demostramos que al pasar a ángulos suplementarios se invierte la relación de orden:

Teorema 4.24 $a - b - a' \wedge a \neq b \neq a' \wedge d - e - d' \wedge d \neq e \neq d'$

$$\rightarrow (\widehat{abd} \leq \widehat{def} \leftrightarrow \widehat{d'ef} \leq \widehat{a'bc}).$$

DEMOSTRACIÓN: Observemos que en realidad basta probar una implicación. Supongamos que $\widehat{abd} \leq \widehat{def}$. Podemos suponer que $\widehat{def}$ no es llano, pues en tal caso su complementario es nulo y la conclusión es trivial.



Sea $p \in \widehat{def}$ tal que $\widehat{dep} \equiv \widehat{abc}$. Entonces $\widehat{d'ep} \equiv \widehat{a'bc}$. Sea $x \sim_e p \wedge f - x - d$. Por **A7** existe un punto y tal que $e - y - f \wedge d - y - x$. Como $y \sim_e f$, tenemos que $f \in \widehat{d'ep}$, luego concluimos que $\widehat{d'ef} \leq \widehat{d'ep} \equiv \widehat{a'bc}$. ■

Ahora podemos definir los ángulos agudos y obtusos:

Definición 4.25

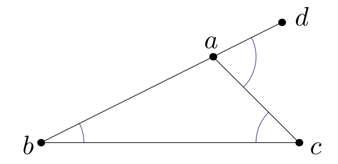
$$\mathrm{Ag}(\widehat{abc}) \leftrightarrow a \neq b \neq c \wedge \bigvee def(Rdef \wedge \widehat{abc} \leq \widehat{def} \wedge \neg \widehat{abc} \equiv \widehat{def}).$$

$$\mathrm{Ob}(\widehat{abc}) \leftrightarrow a \neq b \neq c \wedge \bigvee def(Rdef \wedge \widehat{def} \leq \widehat{abc} \wedge \neg \widehat{abc} \equiv \widehat{def}).$$

4.3 Triángulos

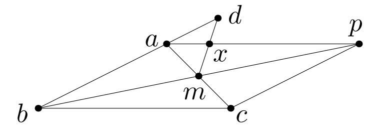
Nos ocupamos ahora de los resultados básicos sobre triángulos. Empezamos demostrando que un ángulo interno de un triángulo es menos que el ángulo externo de otro cualquiera de sus vértices. En general, cuando digamos que un segmento o un ángulo es menor que otro habrá que entenderlo como que es menor o igual, pero no congruente.

Teorema 4.26 $\neg\mathrm{Col}(abc) \wedge b - a - d \wedge d \neq a \rightarrow \widehat{acb} < \widehat{cad} \wedge \widehat{abc} < \widehat{cad}$.



Demostración: Basta probar que $\widehat{acb} < \widehat{cad}$, pues invirtiendo los papeles de b y c obtenemos que $\widehat{acb}$ es menor que el ángulo opuesto por el vértice a $\widehat{cad}$, que sabemos que es congruente con éste.

Sea $m = M(ac)$ y *seap* $= S_m b$. Aplicando S_m obtenemos que $(a, c, b) \equiv (c, a, p)$, luego $\widehat{acb} \equiv \widehat{cap}$. Por **A7** existe un punto x tal que $m - x - d \wedge a - x - p$. Entonces $p \in \widehat{cad}$, luego $\widehat{abc} \leq \widehat{cad}$.



Falta probar que los ángulos no son iguales. Para ello vemos que $p \sim_{ac} d$, pues ambos puntos están separados de b por la recta. Si fuera $\widehat{acb} \equiv \widehat{cad}$, también tendríamos que $\widehat{cap} \equiv \widehat{cad}$, y el teorema 4.15 implica que $p \sim_a d$. En particular $p \in ad$, pero entonces sería $m = a$, luego $c = a$, contradicción. ■

Como consecuencia, un triángulo tiene a lo sumo un ángulo recto u obtuso:

Teorema 4.27 $\neg\mathrm{Col}(abc) \wedge (Rbac \vee \mathrm{Ob}(\widehat{bac})) \to \mathrm{Ag}(\widehat{abc}) \wedge \mathrm{Ag}(\widehat{acb})$.

Demostración: Si d es como en el teorema anterior, entonces $\widehat{cad}$ es recto o agudo, luego los otros dos ángulos, que son menores, son agudos. ■

Un triángulo con dos lados iguales tiene dos ángulos iguales; un ángulo de un triángulo es menor que otro si y sólo si su lado opuesto es menor que el del otro:

Teorema 4.28 *Se cumple:*

1. $\neg\mathrm{Col}(abc) \to (\overline{ab} \equiv \overline{ac} \leftrightarrow \widehat{acb} \equiv \widehat{abc})$,
2. $\neg\mathrm{Col}(abc) \to (\overline{ab} < \overline{ac} \leftrightarrow \widehat{acb} < \widehat{abc})$.

Demostración: La implicación $\overline{ab} \equiv \overline{ac} \to \widehat{acb} \equiv \widehat{abc}$ se sigue inmediatamente de las propiedades de la congruencia de ángulos. Veamos ahora que $\overline{ab} < \overline{ac} \to \widehat{acb} < \widehat{abc}$. Por la definición de orden entre segmentos existe un punto c' tal que $a - c' - c \wedge \overline{ac'} \equiv \overline{ab}$. Como la desigualdad es estricta, $c' \neq c$. Entonces $c' \in \widehat{abc}$, luego $\widehat{acb} < \widehat{ac'b} \equiv \widehat{abc'} \leq \widehat{abc}$, donde hemos usado el teorema anterior, la implicación ya probada y la definición del orden entre ángulos.

Claramente entonces $\overline{ab} \leq \overline{ac} \to \widehat{acb} \leq \widehat{abc}$, luego $\widehat{abc} < \widehat{acb} \to \overline{ac} < \overline{ab}$, que es la implicación contraria con otras letras.

Sólo falta probar que $\widehat{acb} \equiv \widehat{abc} \to \overline{ab} \equiv \overline{ac}$, pero si $\neg\overline{ab} \equiv \overline{ac}$, entonces $\overline{ab} < \overline{ac} \vee \overline{ac} < \overline{ab}$, luego, por la parte ya probada, $\widehat{acb} < \widehat{abc} \vee \widehat{abc} < \widehat{acb}$, luego $\neg\widehat{acb} \equiv \widehat{abc}$. ■

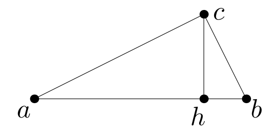
Por ejemplo, si un triángulo tiene un ángulo recto u obtuso, por 4.27 será el mayor de los tres ángulos, luego su lado opuesto será el mayor de los tres lados:

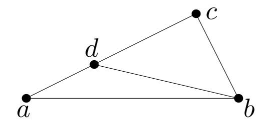
Teorema 4.29 $\neg\mathrm{Col}(abc) \wedge (Rbac \vee \mathrm{Ob}(\widehat{bac})) \to \overline{ab} < \overline{bc} \wedge \overline{ac} < \overline{bc}$.

El teorema siguiente recoge un par de hechos sobre triángulos rectángulos que necesitaremos más adelante:

Teorema 4.30 *Se cumple*

1. $Racb \land ch \perp ab \land h \in ab \to a - h - b \land a \neq h \neq b$,
2. $Racb \land b \neq c \land a - d - c \land a \neq d \neq c \to \widehat{bac} < \widehat{bdc} \land \overline{bd} < \overline{ab}$.





Demostración: 1) Se cumple que $a \neq h \neq b$ porque en otro caso el triángulo $\widehat{abc}$ tendría dos ángulos rectos. Por el teorema anterior aplicado a los tres triángulos rectángulos de la figura izquierda, $\overline{ah} < \overline{ac} < \overline{ab} \land \overline{bh} < \overline{bc} < \overline{ab}$, y el teorema 3.29 implica que $a - h - b$.

2) $\widehat{bac} < \widehat{bdc}$ porque $\widehat{bac} \equiv \widehat{bad}$ y $\widehat{bdc}$ es un ángulo externo del triángulo $\widehat{adb}$, luego basta aplicar el teorema 4.26.

Para probar que $\overline{bd} < \overline{ab}$ basta ver que $\widehat{bad} < \widehat{adb}$, pero el primer ángulo es agudo, porque es un ángulo del triángulo rectángulo $\widehat{abc}$, mientras que el segundo es obtuso, ya que su suplementario $\widehat{bdc}$ es agudo (por la misma razón). ■

Finalmente demostramos los teoremas de congruencia de triángulos. Dos de ellos son inmediatos teniendo en cuenta lo que hemos probado hasta el momento:

Teorema 4.31 (Criterio LLL)

$$\neg\mathrm{Col}(abc) \land (a,b,c) \equiv (a'b'c') \to \widehat{bac} \equiv \widehat{b'a'c'} \land \widehat{abc} \equiv \widehat{a'b'c'} \land \widehat{acb} \equiv \widehat{a'c'b'}.$$

En otras palabras, si dos triángulos tienen sus tres lados iguales, también tienen sus ángulos correspondientes iguales.

Teorema 4.32 (Criterio LAL)

$$\widehat{abc} \equiv \widehat{a'b'c'} \land \overline{ba} \equiv \overline{b'a'} \land \overline{bc} \equiv \overline{b'c'} \to (a,b,c) \equiv (a',b',c').$$

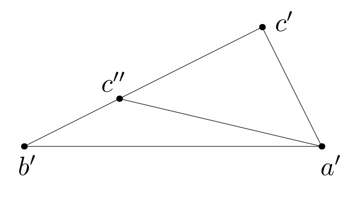
En efecto, sólo hay que probar que $\widehat{ac} \equiv \widehat{a'c'}$, que se sigue inmediatamente de la congruencia de los ángulos.

Teorema 4.33 (Criterio ALA)

$$\neg\mathrm{Col}(abc) \land \widehat{bac} \equiv \widehat{b'a'c'} \land \widehat{abc} \equiv \widehat{a'b'c'} \land \overline{ab} \equiv \overline{a'b'} \to (a,b,c) \equiv (a'b'c').$$

Teorema 4.34 (Criterio AAL)

$$\neg\mathrm{Col}(abc) \land \widehat{bca} \equiv \widehat{b'c'a'} \land \widehat{abc} \equiv \widehat{a'b'c'} \land \overline{ab} \equiv \overline{a'b'} \to (a,b,c) \equiv (a'b'c').$$



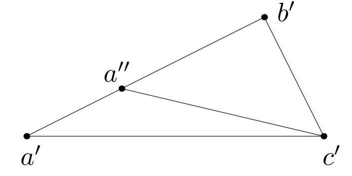
Demostración: Para probar ambos teoremas tomamos un punto $c'' \sim_{b'} c'$ tal que $\overline{b'c''} \equiv \overline{bc}$. Observemos que puede ser $b'-c''-c'$, que es el caso que muestra la figura, o también $b'-c'-c''$. La congruencia $\widehat{abc} \equiv \widehat{a'b'c'}$ implica que $\overline{ac} \equiv \overline{a'c''}$, luego $(a,b,c) \equiv (a'b'c'')$. Basta probar que $c' = c''$.

Caso ALA Tenemos que $\widehat{b'a'c'} \equiv \widehat{bac} \equiv \widehat{b'a'c''}$ y $c'' \sim_{a'b'} c'$. El teorema 4.15 implica que $c'' \sim_{a'} c'$, pero entonces ambos puntos están en las rectas $b'c'$ y $a'c'$, luego $c' = c''$.

Caso AAL Tenemos que $\widehat{b'c'a'} \equiv \widehat{bca} \equiv \widehat{b'c''a'}$. Supongamos que $c' \neq c''$. Si es $b' - c'' - c'$, como muestra la figura, entonces $\widehat{b'c''a'}$ es un ángulo externo del triángulo $\widehat{c''c'a'}$, luego debería ser mayor que $\widehat{b'c'a'}$. Si es $b' - c' - c''$ tendría que darse la desigualdad opuesta (también estricta), luego en ambos casos tenemos una contradicción. ■

Teorema 4.35 (Criterio ALL)

$$\widehat{abc} \equiv \widehat{a'b'c'} \land \overline{ac} \equiv \overline{a'c'} \land \overline{bc} \equiv \overline{b'c'} \land \overline{bc} \leq \overline{ac} \rightarrow (a,b,c) \equiv (a',b',c').$$



Demostración: Sea $a'' \sim_{b'} a'$ de modo que $\overline{b'a''} \equiv \overline{ba}$. La congruencia del ángulo implica que $\overline{ac} \equiv \overline{a''c'}$, luego $(a,b,c) \equiv (a'',b',c')$. Basta probar que $a' = a''$. Supongamos lo contrario.

Tenemos que $\overline{c'a'} \equiv \overline{ca} \equiv \overline{c'a''}$. Puede ocurrir $b' - a'' - a'$ (que es el caso que muestra la figura) o bien $b' - a' - a''$. Distingamos ambos casos:

Si $b'-a''-a'$, suponemos en primer lugar $\neg\mathrm{Col}(abc)$ (las hipótesis no excluyen que los puntos sean colineales). Entonces $\widehat{a''b'c'} < \widehat{a'a''c'}$, porque el segundo ángulo es un ángulo externo del triángulo $\widehat{b'c'a''}$. El teorema 4.28 nos da que $\widehat{a'a''c'} \equiv \widehat{a''a'c'}$, porque forman parte de un triángulo isósceles. Por lo tanto $\widehat{a'b'c'} \equiv \widehat{a''b'c'} < \widehat{a'a''c'} \equiv \widehat{a''a'c'} \equiv \widehat{b'a'c'}$, luego el teorema 4.28 implica que $\overline{a'c'} < \overline{b'c'}$, luego $\overline{ac} < \overline{bc}$, en contra de lo supuesto.

En el caso en que $\mathrm{Col}(abc)$ se tiene que $\widehat{cba}$ es nulo, luego $\widehat{c'b'a'}$ también lo es, luego $\mathrm{Col}(a'b'c')$, luego $c' = Maa''$ (teorema 3.53), luego $a' - c' - a''$, luego $b' - a'' - c'$, luego $\overline{a'c'} \equiv \overline{a''c'} \leq \overline{b'c'}$ y, como $b' \neq a'$ (esto está implícito en la definición de congruencia de ángulos), $\overline{a'c'} < \overline{b'c'}$, luego $\overline{ac} < \overline{bc}$, contradicción.

En el caso $b' - a' - a''$ se razona de forma completamente análoga, intercambiando los papeles de a' y a''. ■

4.4 Variedades afines

Los conceptos de punto, recta y plano se generalizan al concepto de "variedad afín", de modo que los puntos son las variedades afines de dimensión 0, las rectas las de dimensión 1 y los planos las de dimensión 2, pero en esta sección veremos, entre otras cosas, que el proceso que hemos seguido para definir los planos puede generalizarse para definir variedades afines de dimensión arbitraria.

Hay que tener presente, no obstante, que una cosa es definir las variedades afines y otra demostrar su existencia. De entre los axiomas que estamos considerando, el único que aporta información sobre la dimensión del espacio es **A8**, que afirma la existencia de tres puntos no colineales, por lo que el espacio tiene al menos dos dimensiones. Ningún otro axioma afirma nada sobre la dimensión del espacio, de modo que la geometría que hemos desarrollado hasta aquí es válida en espacios de dimensión 2, 3, 4 o cualquier otro valor (incluso en espacios de dimensión infinita). En la sección siguiente veremos cómo enunciar axiomas que determinen la dimensión del espacio.

4.4.1 La definición de las variedades afines

Empezamos expresando con una notación uniforme algunos de los conceptos y resultados que hemos definido o demostrado para puntos, rectas y planos.

Diremos que unos puntos son *afínmente independientes* si cumplen:

- $I^0(a_0) \leftrightarrow a_0 = a_0$ (todo punto es afínmente independiente).
- $I^1(a_0, a_1) \leftrightarrow a_0 \neq a_1$ (todo par de puntos distintos son afínmente independientes).
- $I^2(a_0, a_1, a_2) \leftrightarrow \neg\mathrm{Col}(a_0a_1a_2)$ (tres puntos son afínmente independientes si no son colineales).
- $I^3(a_0, a_1, a_2, a_3) \leftrightarrow \neg\mathrm{Cop}(a_0a_1a_2a_3)$ (cuatro puntos son afínmente independientes si no son coplanares).

Llamaremos *variedades afines de dimensión* 0 a los puntos (o, más precisamente, a los lugares geométricos que constan de un único punto), *variedades afines de dimensión* 1 a las rectas y *variedades afines de dimensión* 2 a los planos. Más precisamente, definimos los lugares geométricos siguientes:

- $A^0(a_0) = \{x \mid x = a_0\}$ (la variedad afín de dimensión 0 generada por el punto a_0 es el lugar geométrico formado por a_0).
- $A^1(a_0, a_1) = \{x \mid I^1(a_0, a_1) \wedge x \in a_0a_1\}$ (la variedad afín de dimensión 1 generada por los puntos independientes a_0 y a_1 es la recta a_0a_1).
- $A^2(a_0, a_1, a_2) = \{x \mid I^2(a_0, a_1, a_2) \wedge x \in a_0a_1a_2\}$) (la variedad afín de dimensión 2 generada por los puntos independientes a_0, a_1, a_2 es el plano $a_0a_1a_2$).

Con estas definiciones podemos reformular así algunos hechos que conocemos:

A) *Si* $I^n(a_0, \ldots, a_n)$*, existe una única variedad afín de dimensión* n *que contiene a* $a_0, \ldots, a_n$*, y ésta es concretamente* $A^n(a_0, \ldots, a_n)$.

(Lo tenemos probado para $n = 1, 2$ y es trivialmente cierto para $n = 0$.)

B) $I^n(a_0, \ldots, a_n)$ *si y sólo si no existen* $x_0, \ldots, x_k$ *con* $k < n$ *de manera que* $I^k(x_0, \ldots, x_k) \land a_0, \ldots, a_n \in A^k(x_0, \ldots, x_k)$.

($n + 1$ puntos son afínmente independientes si y sólo si no están contenidos en una variedad afín de dimensión menor que n. Esto es cierto por definición para $n = 1, 2, 3$.)

C) *Para* $k \leq n$*, si* $I^k(x_0, \ldots, x_k) \land I^n(a_0, \ldots, a_n) \land x_0, \ldots, x_k \in A^n(a_0, \ldots, a_n)$*, entonces* $A^k(x_0, \ldots, x_k) \subset A^n(a_0, \ldots, a_n)$.

(Para $k = 0$ es trivial, para $k = n$ es lo mismo que **A)** y para $k = 1$, $n = 2$ se trata de que si un plano contiene dos puntos, entonces contiene la recta que pasa por ellos. Por lo tanto, lo tenemos probado para $n = 0, 1, 2$.)

D) $\bigvee a_0 \cdots a_n \, I^n(a_0, \ldots, a_n)$.

(Para $n = 0$ afirma la existencia de un punto, para $n = 1$ la existencia de dos puntos y para $n = 2$ la existencia de tres puntos no colineales, lo cual es el axioma **A8**, luego lo tenemos probado para $n = 0, 1, 2$.

Seguidamente extraemos algunas consecuencias de estas cuatro propiedades:

- La propiedad **A)** implica que $A^n(a_0, \ldots, a_n)$ no depende de la ordenación de los puntos, pues es la única variedad afín que los contiene a todos y esto no depende del orden.

- La propiedad **B)** implica que $I^n(a_0, \ldots, a_n)$ tampoco depende del orden de los puntos.

- $I^k(a_0, \ldots, a_k) \land a_{k+1} \notin A^k(a_0, \ldots, a_k) \to I^{k+1}(a_0, \ldots, a_{k+1})$.

  En efecto, si existiera una variedad afín $A^r(x_0, \ldots, x_r)$ con $r \leq k$ tal que $a_0, \ldots, a_{k+1} \in A^r(x_0, \ldots, x_r)$, entonces $r = k$, porque $a_0, \ldots, a_k$ son afínmente independientes (por **B)**), y $A^k(a_0, \ldots, a_k) = A^k(x_0, \ldots, x_k)$ (por **A)**), luego $a_{k+1} \in A^k(a_0, \ldots, a_k)$, en contra de lo supuesto.

  Observemos ahora que si (según **D)**) los puntos $a_0, \ldots, a_n$ son afínmente independientes y $I(x_0, \ldots, x_k)$ con $k < n$, entonces $A^k(x_0, \ldots, x_k)$ no puede contener todos los puntos a_i (por **B)**), luego siempre podremos tomar $x_{k+1} = a_i$, para un i adecuado, de modo que $x_{k+1} \notin A^k(x_0, \ldots, x_k)$, luego $I^{k+1}(x_0, \ldots, x_{k+1})$.

  En otras palabras: un conjunto de $k + 1$ puntos afínmente independientes con $k < n$ siempre puede extenderse hasta un conjunto de $n + 1$ puntos afínmente independientes. Además los puntos añadidos siempre pueden extraerse de cualquier conjunto prefijado de $n + 1$ puntos afínmente independientes. En particular:

- Para $k < n$, se cumple: $A^k(x_0, \ldots, x_k) \subset A^n(a_0, \ldots, a_n) \rightarrow$

$$\bigvee x_{k+1} \cdots x_n \in A^n(a_0, \ldots, a_n)\ A^n(a_0, \ldots, a_n) = A^n(x_0, \ldots, x_n).$$

- $I^{k+1}(a_0, \ldots, a_{k+1}) \rightarrow I^k(a_0, \ldots, a_k)$.

  En efecto, esto equivale a que $\neg I^k(a_0, \ldots, a_k) \rightarrow \neg I^{k+1}(a_0, \ldots, a_{k+1})$. Si se cumple que $a_0, \ldots, a_k$ son afínmente dependientes, existe una variedad afín $A = A^r(x_0, \ldots, x_r)$ tal que $a_0, \ldots, a_k \in A$ con $r < k$. Si también $a_{k+1} \in A$, entonces $\neg I^{k+1}(a_0, \ldots, a_{k+1})$, como queríamos probar, y en caso contrario $I^{r+1}(x_0, \ldots, x_k, a_{k+1})$ y, por **C)**, tenemos la inclusión $A^r(x_0, \ldots, x_k) \subset A^{r+1}(x_0, \ldots, x_k, a_{k+1})$, luego concluimos que $a_0, \ldots, a_{k+1} \in A^{r+1}(x_0, \ldots, x_k, a_{k+1})$ con $r + 1 < k + 1$, luego también $\neg I^{k+1}(a_0, \ldots, a_{k+1})$.

  De aquí se sigue que todo subconjunto de un conjunto afínmente independiente es afínmente independiente. Más aún, combinando el punto anterior con el tercero tenemos:

- $I^{k+1}(a_0, \ldots, a_{k+1}) \leftrightarrow I^k(a_0, \ldots a_k) \wedge a_{k+1} \notin A^k(a_0, \ldots, a_k)$.

- Si la intersección de dos variedades afines no es vacía, entonces es una variedad afín.

  En efecto, sean A y B dos variedades afines de dimensiones $k \leq r$, respectivamente. Supongamos que existe un punto $x_0 \in A \cap B$. Si es el único, entonces $A \cap B = A^0(x_0)$ es una variedad afín.

  Si existe $x_1 \in A \cap B$ distinto de x_0, entonces $A^1(x_0, x_1) \subset A \cap B$ por **C)**. Si no se da la igualdad, existe un $x_2 \in A \cap B \setminus A^1(x_0, x_1)$, con lo que $I^2(x_0, x_1, x_2)$ y $A^2(x_0, x_1, x_2) \subset A \cap B$, de nuevo por **C)**.

  Así vamos obteniendo una sucesión $x_0, x_1, x_2, \ldots$ de puntos afínmente independientes y, si no se ha dado la igualdad $A^i(x_0, \ldots, x_i) = A \cap B$ para ningún $i < k$, llegamos a que $A^k(x_0, \ldots, x_k) \subset A \cap B$, pero ahora necesariamente $A = A^k(x_0, \ldots, x_k)$ por **A)**, pues ambos miembros son variedades afines de dimensión k que contienen a $x_0, \ldots, x_k$. Por lo tanto $A \subset B$ y $A \cap B = A$ es una variedad afín.

Pasamos ya a definir inductivamente las variedades afines según el plan siguiente:

Suponemos definidas las variedades afines hasta dimensión n de modo que se cumplan las propiedades **A)**, **B)**, **C)** y **D)** (y, por consiguiente, todas las consecuencias que acabamos de extraer de ellas).

Definimos $I^{n+1}(a_0, \ldots, a_{n+1})$ mediante la propiedad **B)**, de modo que ésta se cumple para $n + 1$ por definición.

Suponemos que se cumple la propiedad **D)** para $n + 1$, es decir, suponemos que existen $n + 2$ puntos afínmente independientes.

Ahora vamos a definir el concepto de variedad afín de dimensión $n+1$ y probaremos que se cumplen las propiedades **A)** y **C)**.

En lo sucesivo supondremos que A es una variedad afín de dimensión n con $n \geq 2$, es decir, un lugar geométrico de la forma $A^n(a_0, \ldots, a_n)$, aunque los puntos a_i serán irrelevantes.

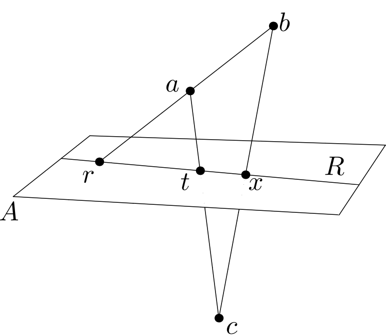
Definición 4.36 $a - A - b \leftrightarrow a \notin A \land b \notin A \land \bigvee t \in A\ a - t - b.$

Notemos que esta definición coincide en los casos $n = 0, 1$ con la que ya teníamos definida para puntos y rectas.

Obviamente $a - A - b \leftrightarrow b - A - a$.

El teorema siguiente generaliza al teorema 3.71:

Teorema 4.37 $a - A - c \land r \in A \to \bigwedge b(a \sim_r b \to b - A - c).$



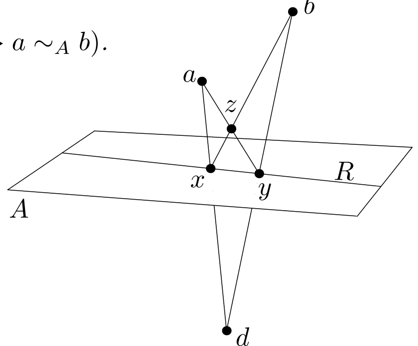
Demostración: Por hipótesis existe un punto $t \in A$ tal que $a - t - c$. Si $t \neq r$, llamamos $R = rt$ y en caso contrario tomamos cualquier recta $R \subset A$ tal que $r \in R$ (aquí usamos la propiedad **B)**).

Por definición $a - R - c \land a \sim_R c$ y por el teorema 3.71 se cumple $b - R - c$, luego existe un $x \in R$ tal que $b - x - c$, luego $b - A - c$. ■

Definición 4.38 $a \sim_A b \leftrightarrow \bigvee c(a - A - c \land b - A - c).$

Nuevamente, esta definición generaliza a las que ya teníamos para $n = 0, 1$. El teorema siguiente generaliza al teorema 3.74:

Teorema 4.39 $a - A - c \to (b - A - c \leftrightarrow a \sim_A b).$



Demostración: La implicación $\Rightarrow$ es inmediata por definición. Supongamos que $a - A - c \land a \sim_A b$. Lo segundo significa que existen puntos d y $x, y \in A$ tales que $d - x - a \land d - y - b$. Sea $R \subset A$ una recta tal que $x, y \in R$.

A partir de aquí la situación es la misma que en el teorema 3.74. Como allí se prueba que existe un punto z tal que $x - z - b \land y - z - a \land z \notin R$. Esto nos da que $a \sim_y z \land z \sim_x b \land a - A - c$. El teorema anterior implica que $z - A - c$ y en una segunda aplicación que $b - A - c$. ■

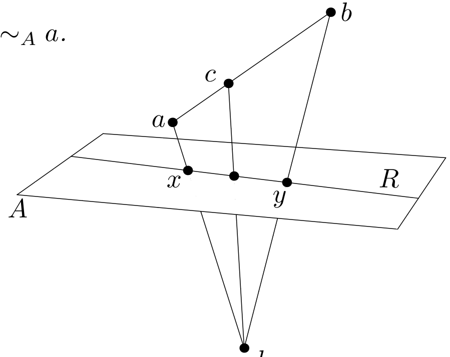
Las propiedades siguientes son todas elementales, y se prueban igual que en el caso $n = 1$:

Teorema 4.40 *Se cumple:*

1. $a - A - b \rightarrow \neg a \sim_A b$,
2. $a \notin A \rightarrow \bigvee c\ a - A - c$,
3. $a \sim_A b \rightarrow b \sim_A a$,
4. $a \sim_A b \wedge b \sim_A c \rightarrow a \sim_A c$.

El teorema siguiente generaliza al teorema 3.76:

Teorema 4.41 $a \sim_A b \wedge a - c - b \rightarrow c \sim_A a$.



DEMOSTRACIÓN: La prueba se reduce a la del teorema 3.76, pues obtenemos dos puntos $x, y \in A$, tomamos una recta $R \subset A$ tal que $x, y \in R$ y a partir de ahí vale el razonamiento bidimensional, como en los teoremas precedentes. ■

El teorema siguiente es el análogo al teorema 3.77 y la prueba no se reduce a la de éste, sino que se demuestra exactamente igual usando las generalizaciones que ya hemos probado de los resultados que se usan en la prueba:

Teorema 4.42 *Se cumple:*

1. $p \in A \wedge \mathrm{Col}(abp) \rightarrow (a - A - b \leftrightarrow a - p - b \wedge a \notin A \wedge b \notin A)$,
2. $p \in A \wedge \mathrm{Col}(abp) \rightarrow (a \sim_A b \leftrightarrow a \sim_p b \wedge a \notin A)$.

Ya podemos definir las variedades afines de dimensión $n+1$:

Definición 4.43 Llamaremos variedades afines de dimensión $n+1$ a los lugares geométricos

$$A^{n+1}(A, r) = \{x \mid x \sim_A r \vee x \in A \vee x - A - r\}, \quad SA^{n+1}(A, r) = \{x \mid x \sim_A r\}.$$

Más explícitamente, la variedad afín generada por $n+2$ puntos afínmente independientes es, por definición,

$$A^{n+1}(a_0, \ldots, a_{n+1}) = A^{n+1}(A^n(a_0, \ldots, a_n), a_{n+1}).$$

El teorema siguiente es análogo al teorema 3.80 y su demostración es formalmente idéntica:

Teorema 4.44 $r - A - r' \rightarrow A^{n+1}(A, r) = SA^{n+1}(A, r) \cup A \cup SA^{n+1}(A, r')$.

Tampoco ofrece ninguna dificultad adaptar la prueba del teorema 3.81 para probar:

Teorema 4.45 $r \notin A \wedge s \notin A \wedge s \in A^{n+1}(A, r) \rightarrow A^{n+1}(A, r) = A^{n+1}(A, s)$.

La generalización del teorema 3.82 es menos obvia:

Teorema 4.46 *Si A es una variedad afín de dimensión n y C es una variedad afín de dimensión $k < n$, $C \subset A$ y $r \notin A$, entonces $A^{k+1}(C, r) \subset A^{n+1}(A, r)$.*

DEMOSTRACIÓN: Si $x \in SA^{k+1}(C, r)$, entonces existen puntos x, y tales que $y - C - r \wedge y - C - x$, luego existen puntos $p, q \in C \subset A$ tales que $y - p - r \wedge y - q - x$, luego $y - A - r \wedge y - A - x$, luego $r \sim_A x$, luego $x \in SA^{n+1}(A, r)$.

Sea $r' - C - r$, lo que implica que $r' \notin A$, pues en otro caso existiría un $c \in C$ tal que $r' - c - r$, con lo que $r \in r'c \subset A$, en contra de lo supuesto. Aplicando a r' lo que hemos probado para r resulta que $SA^{k+1}(C, r') \subset SA^{n+1}(A, r')$. Por lo tanto

$$A^{k+1}(C, r) = SA^{k+1}(C, r) \cup C \cup SA^{k+1}(C, r') \subset$$
$$SA^{n+1}(A, r) \cup A \cup SA^{n+1}(A, r') = A^{n+1}(A, r).$$

■

Supongamos ahora que A y B son dos variedades afines de dimensión $n \geq 2$ tales que su intersección es una variedad afín de dimensión $n - 1$, digamos $C = A^{n-1}(x_0, \ldots, x_{n-1})$. Si $r, r' \in B \setminus C$, entonces $B = A^n(C, r) = A^n(C, r')$.

En efecto, tenemos que B y $A^n(C, r)$ son variedades afines de dimensión n y ambas contienen a $x_0, \ldots, x_{n-1}, r$, que son afínmente independientes porque $x_0, \ldots, x_{n-1}$ lo son por hipótesis y $r \notin C$. Por la propiedad **A)** se tiene la igualdad $B = A^n(C, r)$, e igualmente con r'.

Por el teorema anterior, $r' \in A^n(C, r) \subset A^{n+1}(A, r)$, luego podemos concluir que $A^{n+1}(A, r) = A^{n+1}(A, r')$, por el teorema 4.45.

Esto nos permite definir $A^{n+1}(A, B) = A^{n+1}(A, r)$, para cualquier $r \in B \setminus C$, pues acabamos de probar que la variedad $A^{n+1}(A, r)$ no depende de la elección de r.

Así podemos demostrar el análogo al teorema 3.84:

Teorema 4.47 *Si A y B son dos variedades afines de dimensión n cuya intersección tiene dimensión $n - 1$, entonces*

$$A \subset A^{n+1}(A, B) \wedge B \subset A^{n+1}(A, B) \wedge A^{n+1}(A, B) = A^{n+1}(B, A).$$

DEMOSTRACIÓN: Sea $C = A \cap B$. La inclusión $A \subset A^{n+1}(A, B)$ es inmediata por la definición. Si $b \in B$, entonces, o bien $b \in A$, en cuyo caso $b \in A^{n+1}(A, B)$ por la inclusión anterior, o bien $b \in B \setminus C$, en cuyo caso $b \in A^{n+1}(A, b) = A^{n+1}(A, B)$, por definición. Por lo tanto, también $B \subset A^{n+1}(A, B)$.

Por la simetría en las hipótesis, basta probar que $A^{n+1}(A, B) \subset A^{n+1}(B, A)$.

Pongamos que $A^{n+1}(A, B) = A^{n+1}(A, r)$, con $r \in B \setminus C$, y sea $r' - C - r$. Notemos que $r' \in B \setminus C$, pues existe un $c \in C \subset B$ tal que $r' - c - r$, luego $r' \in cr \subset B$.

Sea $s \in A^{n+1}(A,B)$. Si $s \in A$ o $s \in B$, entonces $s \in A^{n+1}(B,A)$ por las inclusiones ya probadas, así que podemos suponer que $s \notin A \land s \notin B$. En particular $s \in SA^{n+1}(A,r) \lor s \in SA^{n+1}(A,r')$. De nuevo por simetría no perdemos generalidad si suponemos que $s \in SA^{n+1}(A,r)$.

Entonces $s \sim_A r$, luego $r' - A - s$, luego existe un $t \in A$ tal que $r' - t - s$. No puede ser $t \in B$, pues entonces $t \in C$, luego $t \neq r'$ y $s \in tr' \subset B$, contradicción.

Así pues, $t \notin B$, luego $r \neq r'$ (pues $r' \in B$) y podemos aplicar el teorema 4.46 con $C = \{r'\} \subset B$, lo que nos da la inclusión $r't = A^1(r't) \subset A^{n+1}(B,t)$, luego $s \in r't \subset A^{n+1}(B,t) = A^{n+1}(B,A)$, ya que $t \in A \setminus B$. ■

Pasamos ya a demostrar que una variedad afín de dimensión $n+1$ no depende del orden de sus generadores. Probamos en primer lugar que podemos intercambiar dos de ellos:

Teorema 4.48 $A^{n+1}(A^n(a_0,\ldots,a_{n-1},r'),r) = A^{n+1}(A^n(a_0,\ldots,a_{n-1},r),r')$.

DEMOSTRACIÓN: Hay que entender que estamos suponiendo que los puntos $a_0,\ldots,a_{n-1},r'$ son afínmente independientes, y que $r \notin A^n(a_0,\ldots,a_{n-1},r')$. En particular $a_0,\ldots,a_{n-1}$ también son afínmente independientes, por lo que podemos considerar las variedades

$$A = A^n(a_0,\ldots,a_{n-1},r'), \qquad C = A^{n-1}(a_0,\ldots,a_{n-1}).$$

Como $C \subset A$, también $r \notin C$, por lo que $a_0,\ldots,a_{n-1},r$ son afínmente independientes, luego podemos definir $B = A^n(a_0,\ldots,a_{n-1},r)$.

Por construcción $C \subset A \cap B$, pero tiene que darse la igualdad, ya que si existiera un punto $x \in (A \cap B) \setminus C$, entonces los puntos $a_0,\ldots,a_{n-1},x$ serían afínmente independientes y $A^n(C,x) \subset A \cap B$, y las tres variedades tienen dimensión n, luego por la unicidad de la propiedad **A)**, podríamos concluir que $A = A^n(C,x) = B$, luego $r \in A$, en contra de lo supuesto.

Así pues, $C = A \cap B$. En particular $r' \notin B$, pues en caso contrario $r' \in C$ y los generadores de A no serían afínmente independientes. Por el teorema anterior $A^{n+1}(A,r) = A^{n+1}(A,B) = A^{n+1}(B,A) = A^{n+1}(B,r')$. ■

Ahora sólo es cuestión de ir permutando:

Teorema 4.49 *Si S es una variedad afín de dimensión $n+1$ y $a_0,\ldots,a_{n+1} \in S$ son puntos afínmente independientes, entonces $S = A^{n+1}(a_0,\ldots,a_{n+1})$.*

DEMOSTRACIÓN: En principio $S = A^{n+1}(A,r)$, para cierta variedad afín A de dimensión n y cierto $r \notin A$. Digamos que $A = A^n(x_0,\ldots,x_n)$. Si $a_0 \notin A$, entonces, por el teorema 4.45, tenemos que $S = A^{n+1}(A,a_0)$, y por el teorema anterior llegamos a que

$$S = A^{n+1}(A^n(x_0,\ldots,x_{n-1},a_0),x_n),$$

luego podemos suponer que $a_0 \in A$.

Como todo conjunto afínmente independiente se puede completar dentro de una variedad, podemos expresar $A = A^n(a_0, x_1, \ldots, x_n)$. Si $a_1 \notin A$, podemos intercambiar igualmente a_1 con x_n para concluir que

$$S = A^{n+1}(A^n(a_0, x_1, \ldots, x_{n-1}, a_1), x_n),$$

luego podemos suponer que $a_0, a_1 \in A$.

Repitiendo este razonamiento llegamos a que $S = A^{n+1}(A^n(a_0, \ldots, a_n), r)$, y ahora necesariamente $a_{n+1} \notin A$, pues A no puede contener $n + 1$ puntos afínmente independientes, luego el teorema 4.45 nos da finalmente que $S = A^{n+1}(a_0, \ldots, a_{n+1})$. ■

Con esto queda probado que las variedades afines de dimensión $n+1$ cumplen la propiedad **A)**, y la propiedad **C)** se demuestra con la misma técnica empleada en la prueba del teorema anterior:

Si $x_0, \ldots, x_k \in S$ son puntos afínmente independientes, con $k \leq n$ (el caso $k = n + 1$ es el teorema anterior) entonces $S = A^{n+1}(A, r)$, donde podemos suponer que $x_0, \ldots, x_k \in A$, luego por la propiedad **C)** para dimensión n, resulta que $A^k(x_0, \ldots, x_k) \subset A \subset S$.

Así tenemos definido el concepto de variedad afín de dimensión n y el concepto de conjunto de puntos afínmente independientes para cualquier dimensión y cualquier número de puntos, pero hay que tener presente que para definir las variedades afines de dimensión n hemos tenido que suponer la propiedad **D)** para dimensión n, es decir, la existencia de $n + 1$ puntos afínmente independientes. Esto se debe a que, como ya habíamos observado, a partir de nuestros axiomas no podemos demostrar que existan variedades afines de dimensión mayor que 2. (Ni siquiera podemos probar que el espacio no sea el único plano.)

4.4.2 Resultados adicionales sobre variedades afines

Aunque la construcción de las variedades afines ha sido un tanto sofisticada, tienen una caracterización muy simple:

Teorema 4.50 *Sea A una variedad afín y $B \subset A$ un lugar geométrico no vacío y cerrado para rectas, es decir, tal que si $x, y \in S$ son dos puntos distintos, entonces $xy \subset B$. Entonces B es una variedad afín.*

Demostración: Tomamos $x_0 \in B$. Si $B = \{x_0\} = A^0(x_0)$, entonces es una variedad afín. En caso contrario podemos tomar un punto $x_1 \in B \setminus \{x_0\}$. Por hipótesis $x_1x_0 = A^1(x_0, x_1) \subset B$. Si se da la igualdad, ya tenemos que B es una variedad afín. En caso contrario tomamos $x_2 \in B \setminus A^1(x_0, x_1)$.

En general, supongamos que hemos llegado a una sucesión $x_0, \ldots, x_k$ de puntos afínmente independientes tales que que $A_k = A^k(x_0, \ldots, x_k) \subset B$, pero no se da la igualdad. Entonces podemos tomar $x_{k+1} \in B \setminus A^k(x_0, \ldots, x_k)$, con lo que $I^{k+1}(x_0, \ldots, x_{k+1})$ y vamos a probar que

$$A^{k+1}(x_0, \ldots, x_{k+1}) = A^{k+1}(A_k, x_{k+1}) \subset B.$$

Para ello tomamos un punto p tal que $p - A_k - x_{k+1}$. Esto significa que existe un $v \in A_k$ tal que $p - v - x_{k+1}$ y, como $v, x_{k+1} \in B$, por hipótesis $p \in vx_{k+1} \subset B$.

Si $u \in A^{k+1}(A_k, x_{k+1})$, entonces, por definición de variedad afín, hay tres posibilidades:

- $u \in A_k \subset B$.
- $u \in SA^{k+1}(A_k, x_{k+1})$.

  Esto significa que $p - A_k - u$, luego existe un $u' \in A_k$ tal que $p - u' - u$, luego $u \in pu' \subset B$.
- $u \in SA^{k+1}(A_k, p)$.

  Entonces $x_{k+1} - A_k - u$, y concluimos igualmente que $u \in B$.

Como los puntos $x_0, \ldots, x_k \in A$ son afínmente independientes, la sucesión no puede prolongarse indefinidamente, pues k no puede rebasar la dimensión de A. Por lo tanto, tras un número finito de pasos llegamos a que $B = A^k(x_0, \ldots, x_k)$ es una variedad afín. ■

Más adelante daremos axiomas que garantizarán que el espacio E es una variedad afín, luego el teorema anterior podrá aplicarse siempre con $A = E$, y la conclusión será que las variedades afines son simplemente los lugares geométricos cerrados para rectas.

Veamos ahora que podemos determinar una variedad afín a partir de una sucesión de puntos que no sean necesariamente afínmente independientes.

Teorema 4.51 *Dados puntos $a_0, \ldots, a_n$ (no necesariamente afínmente independientes) existe una variedad afín A (de dimensión $k \leq n$) de manera que $a_0, \ldots, a_n \in A$, es la única variedad de dimensión k que cumple esto y ninguna variedad de dimensión $< k$ cumple lo mismo.*

DEMOSTRACIÓN: Llamamos $x_0 = a_0$. Si existe un $a_i \notin A^0(x_0)$, elegimos uno y lo llamamos x_1, si existe otro $a_i \notin A^2(x_0, x_1)$, elegimos uno y lo llamamos x_2, y así sucesivamente. Tras un número finito de pasos tenemos que llegar a una lista de puntos afínmente independientes $x_0, \ldots, x_k$, con $k \leq n$, formada por parte de los a_i, de modo que $a_0, \ldots, a_n \in A^k(x_0, \ldots, x_k)$. No puede suceder que $a_0, \ldots, a_n$ pertenezcan a una variedad afín de dimensión $< k$, pues eso contradiría la independencia afín de $x_0, \ldots, x_k$, y cualquier variedad afín de dimensión k que contenga a $a_0, \ldots, a_n$ en particular contiene a $x_0, \ldots, x_k$, luego es $A^k(x_0, \ldots, x_k)$. ■

Definición 4.52 Llamaremos $\langle a_0, \ldots, a_n \rangle$ a la variedad afín dada por el teorema anterior y la llamaremos *variedad afín generada* por los puntos $a_0, \ldots, a_n$.

Es obvio que $I^n(a_0,\ldots,a_n) \to \langle a_0,\ldots,a_n\rangle = A^n(a_0,\ldots,a_n)$.

En la prueba del teorema anterior hemos visto que todo generador de una variedad afín contiene un generador afínmente independiente. Teniendo esto en cuenta es inmediato que si A es una variedad afín y $a_0,\ldots,a_n \in A$, entonces $\langle a_0,\ldots,a_n\rangle \subset A$.

Teorema 4.53 *Dadas dos variedades afines A y B existe una variedad afín C tal que $A \subset C$, $B \subset C$, es la única variedad de su misma dimensión que las contiene a ambas y ninguna variedad de dimensión menor cumple lo mismo.*

DEMOSTRACIÓN: Si $A = A^m(a_0,\ldots,a_n)$ y $B = A^n(a_0,\ldots,a_n)$, basta tomar $C = \langle a_0,\ldots,a_n,b_0,\ldots,b_n\rangle$. ■

Definición 4.54 Dadas dos variedades afines A y B definimos su *suma* como la variedad afín $A+B$ dada por el teorema anterior.

Es claro entonces que si C es cualquier variedad que contenga a A y B, entonces $A+B \subset C$. También es claro que $\langle a_0,\ldots,a_n\rangle = \langle a_0\rangle + \cdots + \langle a_n\rangle$.

Observemos que el concepto de dimensión de una variedad lo hemos definido al mismo tiempo que hemos definido las variedades, es decir, una variedad afín tiene dimensión n si es de la forma $A^n(x_0,\ldots,x_n)$, para ciertos puntos $x_0,\ldots,x_n$ afínmente independientes. Explícitamente:

Definición 4.55 Para cada número natural n y cada variedad afín A, definimos la fórmula

$$\dim A = n \leftrightarrow \bigvee x_0 \cdots x_n (I^n(x_0,\ldots,x_n) \land A = A^n(x_0,\ldots,x_n)).$$

Vamos a probar un resultado fundamental sobre dimensiones de variedades, para lo cual probamos primero un caso particular:

Teorema 4.56 *Sean A y B dos variedades afines tales que $C = A \cap B$ no sea vacía. Sea $S = A+B$. Si A tiene dimensión $n-1$, B tiene dimensión k y S tiene dimensión n, entonces C tiene dimensión $k-1$.*

DEMOSTRACIÓN: No puede suceder que $B \subset A$, porque entonces tendríamos que $S = A+B = A$, cuando tienen dimensiones distintas. Por lo tanto C está estrictamente contenida en B, luego su dimensión es $\leq k-1$. Vamos a suponer que es $< k+1$.

Tomemos un punto $s \in B \setminus A$. Sea $R = A(C,s) \subset B$. Entonces la dimensión de R es $\leq k-1$, luego existe un $t \in B \setminus R$. Distinguimos tres casos:

1) $s - A - t$. Entonces existe un punto $q \in A$ ($q \neq s$) tal que $s - q - t$. Como $s, t \in B$, también $q \in B$, luego $q \in C \subset R$ y $s \in R$, luego $t \in R$, contradicción.

2) $s \sim_A t$. Entonces tomamos un s' tal que $s' - C - s$ (en particular $s' - A - s$) y así $s' \in R$, luego podemos razonar como en el caso anterior con s' en lugar de s.

3) $t \in A$. Entonces $t \in C \subset R$, contradicción. ■

En general:

Teorema 4.57 *Si A y B son variedades afines con intersección no vacía, entonces*[1]

$$\dim(A+B) = \dim(A) + \dim(B) - \dim(A \cap B).$$

DEMOSTRACIÓN: Sea $S = A + B$, sea $C = A \cap B$ y pongamos que

$$\dim(S) = n, \qquad \dim(A) = n - m, \qquad \dim(B) = k.$$

Tenemos que probar que $\dim(B) = k - m$.

Si $m = 0$ es trivial, pues entonces $B \subset S = A$, luego $C = B$ y su dimensión es k. Si $m = 1$ la conclusión se sigue del teorema anterior.

Probamos el caso general por inducción sobre m, de modo que lo suponemos cierto para $m \geq 1$ y suponemos ahora que $\dim(A) = n - (m+1)$.

No puede ser $B \subset A$, pues entonces $A = S$, pero no tienen la misma dimensión. Por lo tanto existe un punto $a \in B \setminus A$. Sea $A' = A(A, a)$. Así $\dim(A') = n - m$ y $A' + B = A + B$.

Por otra parte, si $C' = A' \cap B$, tenemos que $C \subset C'$, luego C' no es vacía. Aplicamos la hipótesis de inducción a A' y B, de donde concluimos que $\dim(C') = k - m$.

Ahora observamos que $A + C' = A'$ y $A \cap C' = A \cap A' \cap B = A \cap B = C$. Por lo tanto, podemos aplicar el resultado para $m = 1$, que nos da que

$$n - m = \dim(A') = \dim(A) + \dim(C') - \dim(C) = n - (m+1) + k - m - \dim(C),$$

de donde llegamos a que $\dim(C) = k - (m+1)$, como había que probar. ■

Un caso particular de interés (que, de hecho, se sigue del teorema 4.56) es el siguiente:

Teorema 4.58 *Si P_1 y P_2 son planos contenidos en una variedad afín de dimensión 3 y tienen un punto en común, entonces tienen una recta en común.*

DEMOSTRACIÓN: Si S tiene dimensión 3 y $P_1, P_2 \subset S$, entonces $P_1 + P_2 \subset S$, luego

$$3 \geq \dim(P_1 + P_2) = \dim(P_1) + \dim(P_2) - \dim(P_1 \cap P_2) = 4 - \dim(P_1 \cap P_2),$$

luego $\dim(P_1 \cap P_2) \geq 1$. ■

Para terminar construimos una variedad afín que nos será útil en diversos contextos:

[1] El lector interesado en la lógica (de primer orden) subyacente a la geometría de Tarski debería observar que los números naturales, la aritmética, el razonamiento por inducción de este teorema y el propio concepto de dimensión son todos metamatemáticos, externos a la teoría formal que estamos considerando. Este teorema es en realidad un esquema teoremático en el que las dimensiones aparecen reflejadas en el número de variables con el que se determina cada variedad afín.

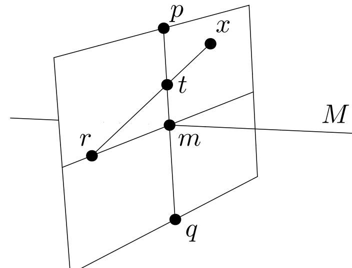
Definición 4.59 Si A es una variedad afín y $p, q \in A$ son dos puntos distintos, definimos

$$M_A(pq) = \{x \mid x \in A \land \overline{xp} \equiv \overline{xq}\}.$$

Así, $M_A(pq)$ es el lugar geométrico formado por los puntos de A que equidistan de los dos puntos dados.

Teorema 4.60 *Si A es una variedad afín de dimensión n y $p, q \in A$ son dos puntos distintos, entonces $M_A(pq)$ es una variedad afín de dimensión $n-1$.*

DEMOSTRACIÓN: Que $M = M_A(pq)$ es una variedad afín se sigue inmediatamente del teorema 4.50, pues claramente el punto medio Mpq está en M (luego no es el conjunto vacío), y si $x, y \in M$ son dos puntos distintos, el teorema 3.19 implica que $xy \subset M$.



Obviamente $M \neq A$, pues $p, q \notin M$, luego la dimensión de M es menor que n. Supongamos que es $k < n-1$. Entonces la dimensión de $A^{k+1}(M, p) \subset A$ es $k+1 < n$, luego podemos tomar un punto $x \in A \setminus A^{k+1}(M, p)$. Sea $m = Mpq \in M$. Como $m, p \in A^{k+1}(M, p)$, también $q \in A^{k+1}(M, p)$, pero $x \notin pq$, pues en caso contrario $x \in A^{k+1}(M, p)$. Por 3.65 existen puntos r y $t \in pq$ tales que $rm \perp pq$ y $r - t - x$.

Por definición de perpendicularidad, $\overline{rp} \equiv \overline{rq}$, luego $r \in M$, pero tenemos que $t \in pq \subset A^{k+1}(M, p)$, luego $x \in rt \subset A^{k+1}(M, p)$, contradicción. ■

4.5 La dimensión del espacio

Ahora es fácil incorporar a la teoría axiomas que determinen la dimensión del espacio. Una posibilidad es (para cualquier número natural $n \geq 2$):

$\mathbf{A8_n}$	$\bigvee a_0 \cdots a_n \; I^n(a_0, \ldots, a_n)$
$\mathbf{A9_n}$	$\neg\bigvee a_0 \cdots a_{n+1} \; I^{n+1}(a_0, \ldots, a_{n+1})$

de modo que $\mathbf{A8_2}$ es equivalente al axioma **A8**. Si tomamos como definición de independencia afín la relación recurrente

$$I^{n+1}(a_0, \ldots, a_{n+1}) \leftrightarrow I^n(a_0, \ldots, a_n) \land a_{n+1} \notin A^n(a_0, \ldots, a_n), \quad n \geq 3.$$

se cumple trivialmente (sin necesidad de apelar a ningún axioma geométrico) que si $k \leq n$ entonces $I^n(a_0, \ldots, a_n) \rightarrow I^k(a_0, \ldots, a_k)$, por lo que, si $2 \leq k \leq n$, se cumple que $\mathbf{A8_n} \rightarrow \mathbf{A8_k}$ y $\mathbf{A9_k} \rightarrow \mathbf{A9_n}$.

Cuando sustituimos el axioma **A8** por $\mathbf{A8_n}$ y añadimos $\mathbf{A9_n}$ (con $n \geq 2$) obtenemos la *Geometría de Tarski* n-dimensional.

Si $a_0, \ldots, a_n$ son puntos afínmente independientes dados por $\mathbf{A8_n}$ y consideramos la variedad afín $A^n(a_0, \ldots, a_n)$, el axioma $\mathbf{A9_n}$ nos da que tiene que ser igual a todo el espacio: $E = A^n(a_0, \ldots, a_n)$, pues si existiera un punto $a_{n+1} \in E \setminus A^n(a_0, \ldots, a_n)$ tendríamos $I^{n+1}(a_0, \ldots, a_{n+1})$.

Así pues, a partir de los axiomas de la Geometría de Tarski n-dimensional se demuestra que el espacio E es una variedad afín de dimensión n.

Por otra parte, es posible introducir axiomas que establezcan que la dimensión del espacio es 2 o 3 sin necesidad de involucrar la definición general de variedad afín o de independencia afín. Por ejemplo, para establecer que el espacio tiene dos dimensiones basta añadir al axioma **A8** el axioma

A9 $p \neq q \land \overline{xp} \equiv \overline{xq} \land \overline{yp} \equiv \overline{yq} \land \overline{zp} \equiv \overline{zq} \rightarrow \mathrm{Col}(xyz)$.

En efecto, lo que afirma este axioma es que si p y q son puntos distintos, entonces $M = M_E(pq)$ es una recta. Partiendo de este axioma, una ligera adaptación de la prueba del teorema 4.60 implica que el espacio E coincide con el plano $P(M, p)$.

Para establecer que el espacio tiene tres dimensiones podemos tomar $\mathbf{A8_3}$, es decir,

$\mathbf{A8_3}$ $\bigvee xyzw(x \neq y \land z \notin xy \land w \notin xyz)$

junto con

$\mathbf{A9_3^*}$ *Si dos planos tienen un punto en común, tienen dos puntos en común.*

Por el teorema 4.58, si el espacio E es una variedad afín de dimensión 3, se cumple $\mathbf{A9_3^*}$. Recíprocamente, si se cumple este axioma no puede haber cinco puntos v, w, x, y, z afínmente independientes, ya que entonces los planos $P_1 = vwx$ y $P_2 = vyz$ sólo tendrían en común el punto v.

En efecto, $P_1 + P_2 = \langle u, v, w, x, y, z \rangle$, luego $\dim(P_1 + P_2) = 4$, y la fórmula del teorema 4.57 nos da que que $\dim(P_1 \cap P_2) = 0$.

Por lo tanto, $\mathbf{A8_3}$ y $\mathbf{A9_3^*}$ equivalen a que el espacio E es una variedad afín de dimensión 3.

En lo sucesivo seguiremos trabajando únicamente con el axioma **A8**, puesto que ninguno de los resultados que vamos a probar dependerá de la dimensión del espacio.

Capítulo V

La geometría euclídea

Introducimos ahora el axioma de las paralelas, que caracteriza a la geometría euclídea. Tal y como indicábamos al final del capítulo anterior, seguiremos trabajando en la teoría determinada por los axiomas **A1**–**A8**, sin suponer ningún axioma sobre la dimensión del espacio.

5.1 El axioma de las paralelas

Definición 5.1 Dos rectas son *paralelas* si son coplanares y, o bien son iguales, o bien no tienen puntos en común:

$$R \parallel S \leftrightarrow \mathrm{Cop}(R, S) \land (R = S \lor \neg \bigvee x(x \in R \land x \in S)),$$

donde Cop indica que las rectas son coplanares, es decir,

$$\mathrm{Cop}(R, S) \leftrightarrow \bigvee xyz(\neg \mathrm{Col}(xyz) \land R \subset xyz \land S \subset xyz).$$

Por ejemplo, dos rectas perpendiculares a una tercera son paralelas:

Teorema 5.2 $\mathrm{Cop}(R, S, T) \land R \perp T \land S \perp T \to R \parallel S$.

Demostración: Sean r y s los puntos de corte de R y S con T. Si $r = s$, entonces $R = S$ por la unicidad de las perpendiculares (teorema 4.17), luego $R \parallel S$. Si $r \neq s$, entonces $R \neq S$ (pues las dos rectas cortan a T en puntos distintos), y si existiera $a \in R \cap S$ entonces el triángulo $\widehat{ars}$ tendría dos ángulos rectos, lo cual es imposible (teorema 3.59). Por lo tanto $R \parallel S$. ■

Como consecuencia, por todo punto dado pasa una paralela a una recta dada:

Teorema 5.3 $\bigvee S(S \parallel R \land a \in S)$.

Demostración: Si $a \in R$ basta tomar $S = R$. Si $a \notin R$, por el teorema 3.63 existe una recta T tal que $R \perp T \land a \in T$. Por 4.17 existe una recta S contenida en el plano $P(R, T)$ tal que $S \perp T \land a \in S$. Entonces R y S son perpendiculares a T en el mismo plano, luego por el teorema anterior $S \parallel R$. ■

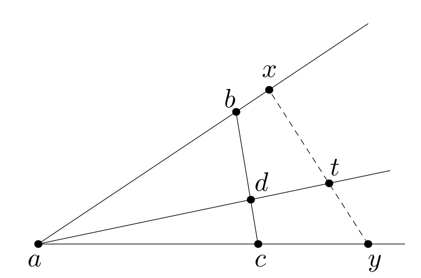
Es evidente que la relación de paralelismo es reflexiva y simétrica:

$$R \parallel R, \qquad R \parallel S \to S \parallel R.$$

En cambio, la transitividad del paralelismo no es demostrable a partir de los axiomas que estamos considerando:

Teorema 5.4 *Las afirmaciones siguientes son equivalentes:*

1. $\overset{1}{\bigvee} S(S \parallel R \land a \in S)$ *(por cada punto existe una única paralela a una recta dada),*
2. $R \parallel S \land S \parallel T \to R \parallel T$ *(transitividad del paralelismo),*
3. $a - d - t \land b - d - c \land a \neq d \to \bigvee xy(a - b - x \land a - c - y \land x - t - y)$.



La última afirmación es un tanto técnica, pero tiene el interés de que sólo aparecen en ella los conceptos primitivos (no definidos) de la teoría.

Demostración: 1) ⇒ 2) Supongamos que $R \parallel S \land S \parallel T$ y distingamos dos casos:

Caso 1: R, S, T son coplanares.

Si existe un punto $a \in R \cap T$ tenemos que R y T son dos paralelas a S por a, luego por 1) $R = T$ y en particular $R \parallel T$.

Caso 2: R, S, T no son coplanares. En particular las tres rectas son distintas dos a dos, pues R y S son coplanares, al igual que S y T.

Llamemos P al plano que contiene a R y S. Como $T \not\subset P$, existe un punto $t \in T \setminus P$. Llamemos $P_R = P(R, t)$ y $P_S = P(S, t)$. Observemos que $P_R \neq P_S$, pues si fueran el mismo plano, éste contendría a R y S, luego sería P, pero entonces $t \in P$.

Por otra parte, $P_R, P_S \subset A^3(P, t)$, que es una variedad de dimensión 3, y $t \in P_R \cap P_S$, luego el teorema 4.58 implica que la intersección $T' = P_R \cap P_S$ es una recta.

Observemos que T' no puede cortar a P, pues si $x \in T' \cap P$ entonces

$$x \in (T' \cap P_R) \cap (T' \cap P_S) = R \cap S,$$

que son paralelas distintas. En particular T' no corta ni a R ni a S y es coplanar con ambas, luego $T' \parallel R \land T' \parallel S$, pero entonces T y T' son paralelas a S que pasan por t, luego 1) implica que $T' = T$, luego $R \parallel T$.

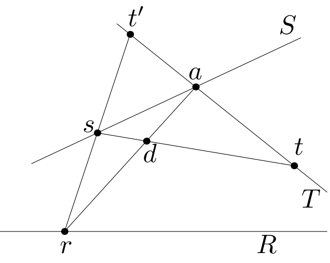
2) ⇒ 3) Si $at = bc$ es fácil probar la conclusión sin usar 2). Supongamos, pues, que las rectas son distintas. Claramente $a \neq t$. Si $t = d$ sirven $x = b$, $y = c$, así que podemos suponer que $t \neq d$, luego $t \notin bc$.

Por el teorema 5.3 existe una recta $R \parallel bc$ tal que $t \in R$. Entonces R está en el plano bct, al cual pertenece también a. En particular R es coplanar con ab, luego si R no cortara a ab sería $R \parallel ab$, luego por la transitividad $ab \parallel bc$, lo cual es absurdo, pues ambas rectas se cortan en b (y no puede ser $ab = bc$, pues entonces $at = bc$). Así pues, existe $x \in R \cap ab$, y el mismo argumento nos da un punto $y \in R \cap ac$.

Como $R = xt = xy$ no corta a bc, tenemos que $x \sim_{ac} t \wedge y \sim_{bc} t$, pero $a - bc - t$, luego $a - bc - x \wedge a - bc - y$, y esto equivale a $a - b - x \wedge a - c - y$.

Por otra parte $t \sim_{ax} d \sim_{ax} c \sim_{ax} y$, e igualmente $t \sim_{by} x$, luego 3.78 nos da que $x - t - y$.

3) ⇒ 1) Supongamos que S y T son paralelas a R por a. Si $a \in R$, necesariamente $S = R = T$, luego podemos suponer que $a \notin R$. Tomemos $r \in R$ y sea $t' \in T$ tal que $r - S - t'$. Esto es posible, pues siempre podemos tomar $t_1, t_2 \in T$ tales que $t_1 - a - t_2$ y uno de los dos sirve.



Sea $s \in S$ tal que $r - s - t'$ y sea $t \in T$ tal que $t' - a - t \wedge a \neq t$. Por el axioma **A7** aplicado al triángulo $\widehat{rat'}$ existe un punto d tal que $s - d - t \wedge r - d - a$. Tiene que ser $s \neq a$, pues en caso contrario $t's = at = T$, luego $r \in T$. Además $a \notin st$, pues en caso contrario $st = at = T$, luego $s \in S \cap T$, luego $s = a$. Por lo tanto $a \neq d$.

Por 3) existen puntos x, y tales que $a - s - x \wedge a - t - y \wedge x - r - y$, pero esto es imposible: por un lado $x - R - y$, pero por otro resulta que ax, ay no cortan a R, luego $x \sim_R a \sim_R y$, contradicción. ■

A partir de aquí tomaremos como axioma (el axioma **A10** de la geometría de Tarski) la afirmación 3) del teorema anterior, y ya conocemos dos enunciados equivalentes. Es fácil probar que también equivale al teorema siguiente:

Teorema 5.5 *Si R, S, T son rectas coplanares, $R \parallel S$ y T corta a R, entonces T también corta a S.*

Demostración: Si T no corta a S, entonces $T \parallel S$, luego por la transitividad del paralelismo $T \parallel R$, contradicción. ■

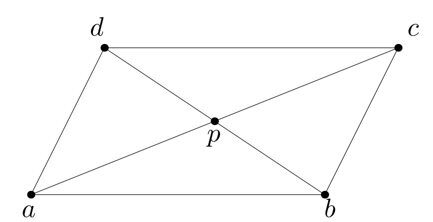
Veamos ahora algunas propiedades de los paralelogramos. Observemos que las dos primeras no requieren **A10**:

Teorema 5.6 *Se cumple:*

1. $p = Mac = Mbd \wedge a \neq b \rightarrow ab \parallel cd$,
2. $\overline{ab} \equiv \overline{cd} \wedge \overline{bc} \equiv \overline{de} \wedge \neg\mathrm{Col}(abc) \wedge b \neq d \wedge \mathrm{Col}(apc) \wedge \mathrm{Col}(bpd) \rightarrow$
   $ab \parallel cd \wedge bc \parallel ad \wedge b - ac - d \wedge a - bd - c$,

3. $\neg\mathrm{Col}(abc) \wedge ab \parallel cd \wedge bc \parallel da \to \overline{ab} \equiv \overline{cd} \wedge \overline{bc} \equiv \overline{de} \wedge b - ac - d \wedge a - bd - c$,

4. $ab \parallel cd \wedge \overline{ab} \equiv \overline{cd} \wedge b - ac - d \to bc \parallel da \wedge \overline{bc} \equiv \overline{da} \wedge a - bd - c$.



Demostración: 1) Si $\mathrm{Col}(abp)$, entonces $ab = cd$ y la conclusión es trivial. Supongamos, pues que $\neg\mathrm{Col}(abp)$, y sea R la perpendicular a ab por p. Aplicando S_p obtenemos que $R \perp cd$, luego $ab \parallel cd$ por el teorema 5.2.

2) Por el teorema 3.54 tenemos que $p = Mac = Mbd$, y basta aplicar el apartado anterior.

3) Sea $p = Mac$ y sea $d' = S_p b$. Entonces, aplicando que S_p conserva las congruencias, vemos que $\overline{ab} \equiv \overline{cd'} \wedge \overline{bc} \equiv \overline{d'a}$. Como $p = Mac = Mbd'$, el apartado 1) nos da que $ab \parallel cd'$, luego $cd' \parallel cd$, luego $cd' = cd$ e igualmente $ad = ad'$, Entonces d y d' son ambos la intersección de ad con cd, luego $d = d'$ y la conclusión es inmediata.

4) Como $b - ac - d$, sabemos que $\neg\mathrm{Col}(abd)$. Sea b' tal que $b' - a - b \wedge b' \neq a$. Tenemos que $d \sim_{ab} c$ porque las rectas ab y cd son paralelas, luego una no puede separar puntos de la otra. Por otro lado $b' - ac - b \wedge d - ac - b$, luego $b' \sim_{ac} d$. El teorema 3.78 implica que $b' - ad - c$, lo que, unido a $b' - ad - b$, nos da que $b \sim_{ad} c$.

Sea R la paralela a ad que pasa por b. Como corta a ab, también tiene que cortar a la paralela dc en un punto c'. Por 3) concluimos que $\overline{dc'} \equiv \overline{ab}$, luego $\overline{dc'} \equiv \overline{dc}$ y además $d' \sim_{ad} b$ (porque bc' es paralela a ad) y $b \sim_{ad} c$, luego $c \sim_{ad} c'$, luego $c \sim_d c'$. El teorema 3.35 implica que $c = c'$, luego $ad \parallel bc$ y concluimos aplicando 3). ■

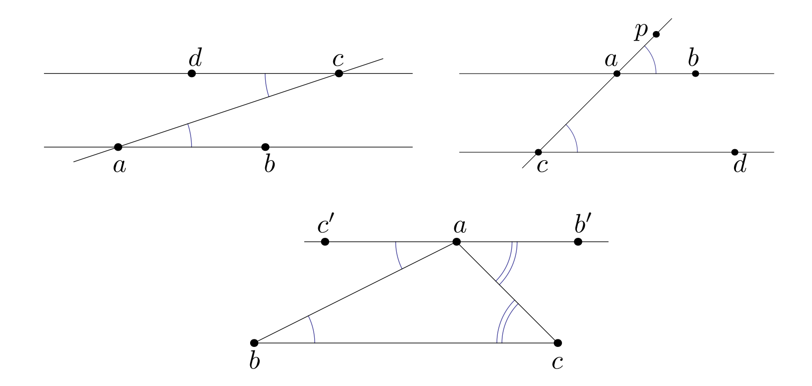
He aquí otras consecuencias del axioma de las paralelas (que de hecho son afirmaciones equivalentes). La primera es el quinto postulado de Euclides. La tercera afirma esencialmente que la suma de los ángulos de un triángulo es igual a un ángulo llano, aunque no podemos enunciarla así porque no hemos definido la suma de ángulos:

Teorema 5.7 *Se cumple:*

1. $b - ac - d \to (ab \parallel cd \leftrightarrow \widehat{bac} \equiv \widehat{dca})$,

2. $a \sim_p c \wedge b \sim_{pa} d \to (ab \parallel cd \leftrightarrow \widehat{bap} \equiv \widehat{dcp})$,

3. $\neg Col(abc) \to \bigvee b'c'(b' - a - c' \wedge b - ac - b' \wedge c - ab - c' \wedge \widehat{abc} \equiv \widehat{bac'} \wedge \widehat{acb} \equiv \widehat{cab'})$.



Demostración: Para probar 1) no perdemos generalidad si suponemos que $\overline{ab} \equiv \overline{cd}$, y entonces podemos aplicar el teorema anterior. La propiedad 2) se deduce de 1) considerando el ángulo opuesto por el vértice de $\widehat{bap}$. Por último 3) es consecuencia de 1). ■

Vamos a necesitar un resultado sobre planos paralelos. El paralelismo de planos se define como sigue:

Definición 5.8 Diremos que dos planos P_1 y P_2 son *paralelos* si están contenidos en una misma variedad afín tridimensional y no tienen puntos en común. Lo representaremos por $P_1 \parallel P_2$.

Obviamente, si admitimos axiomas que afirmen que el espacio es una variedad afín tridimensional, entonces la definición anterior se reduce a que dos planos son paralelos si y sólo si son disjuntos, pero en ausencia de tales axiomas hay que exigir que ambos estén contenidos en una misma variedad tridimensional igual que en la definición de rectas paralelas exigimos que sean coplanares.

Teorema 5.9 *Dados dos planos P_1 y P_2, las afirmaciones siguientes son equivalentes:*

1. $P_1 \parallel P_2$,
2. *Para todo plano Q, si $R = P_1 \cap Q$ es una recta y $P_2 \cap Q \neq \varnothing$, entonces $P_2 \cap Q$ es una recta paralela a R.*
3. *Existen dos pares de rectas secantes $R_1, R_2 \subset P_1$ y $S_2, S_2 \subset P_2$ tales que $R_1 \parallel S_1$ y $R_2 \parallel S_2$.*

Demostración: 1) ⇒ 2) Si $P_1 = P_2$ la conclusión es trivial, luego podemos suponer que $P_1 \cap P_2 = \varnothing$. Sea A una variedad afín tridimensional que contenga a P_1 y P_2. Sea $p \in P_2 \cap Q$. Entonces $R \subset A \wedge p \in A$ (pero $p \notin R$), luego $Q = P(R, p) \subset A$ y por el teorema 4.58 tenemos que $S = P_2 \cap Q$ es una recta. Como $R, S \subset Q$, ambas rectas son coplanares, y $R \cap S = \varnothing$, pues en caso contrario la intersección estaría en $P_1 \cap P_2 = \varnothing$. Por lo tanto $R \parallel S$.

2) $\Rightarrow$ 3) Podemos suponer que $P_1 \neq P_2$. Tomamos un punto $p \in P_2 \setminus P_1$ y $R_1, R_2 \subset P_1$ dos rectas secantes cualesquiera. Por 2), los planos $P(R_1, p)$ y $P(R_2, p)$ cortan a P_2 en rectas S_1 y S_2, respectivamente, que contienen a p, luego son secantes (no pueden ser iguales, ya que entonces R_1 y R_2 tendrían que ser paralelas). Por lo tanto se cumple 3).

3) $\Rightarrow$ 1) Sean $p \in R_1 \cap R_2$ y $q \in S_1 \cap S_2$. Si $p = q$, entonces $R_1 = S_1$ y $R_2 = S_2$, luego $P_1 = P_2$. Por lo tanto, podemos suponer que $p \neq q$. Si $R_1 = S_1$, entonces $P(R_2, S_2)$ contiene a p, q, luego a $R_1 = pq$, luego de nuevo $P_1 = P(R_2, S_2) = P_2$. Así pues, podemos suponer que $R_1 \neq S_1$ y, análogamente, que $R_2 \neq S_2$.

Sean $Q_1 = P(R_1, S_1)$, $Q_2 = P(R_2, S_2)$. Así $Q_1 \cap Q_2 = pq$. (Notemos que si fuera $Q_1 = Q_2$ también tendríamos $P_1 = P_2$.) Entonces $A = Q_1 + Q_2$ es una variedad afín de dimensión 3 por el teorema 4.57, y ciertamente $P_1, P_2 \subset A$.

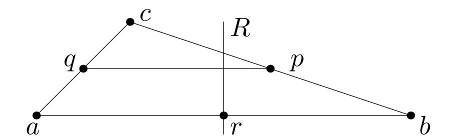
Falta probar que $P_1 \cap P_2 = \varnothing$. En caso contrario (y suponiendo además que $P_1 \neq P_2$) el teorema 4.58 implica que $C = P_1 \cap P_2$ es una recta. Como no puede ser paralela tanto a R_1 como a R_2, podemos suponer que no es paralela a R_1, y por lo tanto tampoco a S_1. Pero $C, R_1 \subset P_1$ son coplanares, luego secantes y, más aún, P_1 es el único plano que contiene a ambas. Igualmente, P_2 es el único plano que contiene a C y a S_1. Pero R_1 y S_1 son coplanares, y el único plano que las contiene contiene también a C (porque contiene a sus puntos de corte con R_1 y S_2, luego dicho plano es $P_1 = P_2$, contradicción. ■

5.2 El teorema de Pappos-Pascal

Nuestro objetivo a medio plazo es definir una suma y un producto en cada recta que determinen una estructura de cuerpo, para lo cual necesitaremos dos resultados clásicos: el teorema de Pappos-Pascal y el teorema de Desargues. Aquí nos ocuparemos del primero. De momento no supondremos el axioma de las paralelas.

Teorema 5.10 $\neg\mathrm{Col}(abc) \land p = Mbc \land q = Mca \land r = Mab \rightarrow$

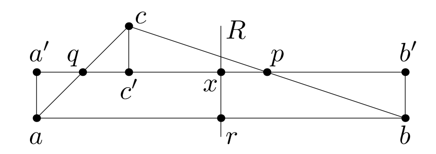
$$\bigvee R \in \mathcal{R}(r \in R \land R \perp ab \land R \perp pq).$$



Por el punto medio de un lado de un triángulo pasa una perpendicular común a dicho lado y a la recta que pasa por los puntos medios de los otros dos lados. En particular dicha recta es paralela al lado.

Demostración: Sea $c' \in pq$ tal que $cc' \perp pq$, es decir, c' es el pie de la perpendicular a pq por c. Sea $a' = S_q c'$ y $b' = S_p c'$. Aplicando S_q obtenemos que $\overline{aa'} \equiv \overline{cc'}$ y aplicando S_p que $\overline{cc'} \equiv \overline{bb'}$. Además, como $cc' \perp c'b'$, al aplicar S_p resulta que $bb' \perp c'b' = pq$. Igualmente $a'a \perp pq$.

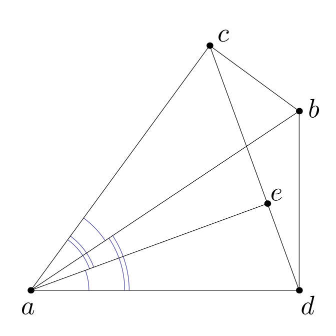
Sea $x = Ma'b'$ y sea R la recta perpendicular a pq que pasa por x y que está contenida en el plano abc (que contiene a todos los puntos que estamos considerando). Entonces $b' = S_R a'$ y llamamos $b'' = S_R a$, de modo que $R(a'b'b'')$, $\overline{aa'} \equiv \overline{b'b''}$ (luego $\overline{bb'} \equiv \overline{b''b'}$) y $b'' \sim_{pq} a$ (porque $b''a \parallel b'a' = pq$, ya que R es una perpendicular común). Pero también $R(a'b'b)$ y $b \sim_{pq} a$, pues $pq \parallel ab$, luego $b \sim_{b'} b''$. Esto implica que $b = b''$, pues son dos puntos en la misma semirrecta de origen b' a la misma distancia de b'.



Por lo tanto $b = S_R a$ y concluimos que $r = Mab \in R$. ■

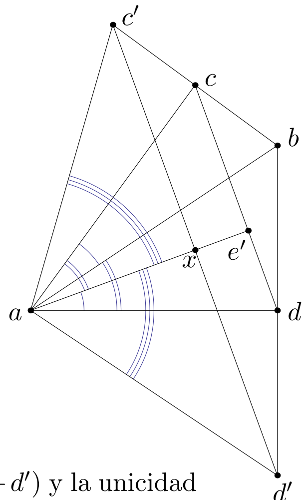
Teorema 5.11 $c - ab - d \wedge Rbca \wedge Rbda \wedge \mathrm{Col}(cde) \wedge ae \perp cd \rightarrow$

$$\widehat{bac} \equiv \widehat{dae} \wedge \widehat{bad} \equiv \widehat{cae} \wedge c - e - d.$$



Si tenemos dos triángulos rectángulos con la hipotenusa en común, la perpendicular a cd por a divide al ángulo $\widehat{dac}$ que son los mismos en que lo divide ab, pero en orden inverso.

DEMOSTRACIÓN: De $c - ab - d$ se sigue inmediatamente que $b \in \widehat{dac}$, y a su vez de aquí que $\widehat{bac} \leq \widehat{dac}$. Esto a su vez implica que existe un punto e' tal que $d - e' - c \wedge \widehat{dae'} \equiv \widehat{bac}$. El teorema 4.19 nos da que $\widehat{e'ac} \equiv \widehat{dab}$. Basta probar que $e' = e$, para lo cual a su vez basta probar que $ae' \perp cd$. Llamemos $R = ae'$.



Sea $c' = S_c b$ y $d' = S_d b$. Las hipótesis sobre los ángulos rectos implican que $\overline{ac'} \equiv \overline{ab} \equiv \overline{ad'}$, luego $\widehat{bac} \equiv \widehat{c'ac}$ y $\widehat{bad} \equiv \widehat{d'ad}$. Usando de nuevo el teorema 4.19 concluimos que $\widehat{c'ae'} \equiv \widehat{e'ad'}$ (pues ambos son la suma de un ángulo marcado con un arco y otro marcado con dos).

Es claro que $c' \neq d'$ (por ejemplo, porque $c' - ab - d'$) y la unicidad del transporte de ángulos implica que la única posibilidad para que

dos ángulos congruentes compartan un lado sin ser iguales es que $c' - R - d'$, y además, como $\overline{ac'} \equiv \overline{ad'}$, llamando x al punto en que $c'd'$ corta a R, se cumple que $\overline{c'x} \equiv \overline{xd'}$, luego $x = Mc'd'$ y $Raxc'$, luego $d' = S_R c'$.

Finalmente aplicamos el teorema anterior al triángulo $\widehat{bc'd'}$ para concluir que R es perpendicular a dc, como había que probar. ■

Ahora necesitamos definir una "trigonometría rudimentaria":

Definición 5.12 Llamaremos *longitud* de un segmento $\overline{ab}$ a

$$[\overline{ab}] = \{(x, y) \mid \overline{xy} \equiv \overline{ab}\}.$$

Observemos que no se trata de un lugar geométrico, pues no es un conjunto de puntos, pero la filosofía es la misma, esta definición (que en sí misma no significa nada), permite interpretar como fórmulas del lenguaje de la geometría de Tarski la fórmula:

$$[\overline{ab}] = [\overline{cd}] \leftrightarrow \overline{ab} \equiv \overline{cd}.$$

Hasta aquí, esto no aporta nada, pero lo interesante es que podemos hablar de "una longitud l" sin necesidad de especificar a y b.

En particular llamaremos *longitud nula* a la longitud $0 = [\overline{aa}]$, para cualquier punto a.

Similarmente definimos la *amplitud* de un ángulo $\widehat{abc}$ como

$$[\widehat{abc}] = \{(x, y, z) \mid a \neq b \neq c \land x \neq y \neq z \land \widehat{xyz} \equiv \widehat{abc}\},$$

de modo que

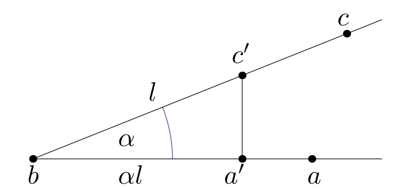
$$[\widehat{abc}] = [\widehat{a'b'c'}] \leftrightarrow \widehat{abc} \equiv \widehat{a'b'c'}.$$

Así, todas las ternas (a, b, c) con $a \sim_b c$ determinan la misma amplitud, que llamaremos *amplitud nula* y representaremos por 0. Igualmente, las ternas con $a - b - c \land a \neq b \neq c$ determinan una misma amplitud que representaremos por π y las ternas con $Rabc$ determinan una misma amplitud que representaremos por $\pi/2$.

Si $l = [\overline{uv}]$ es una longitud y $\alpha = [\widehat{abc}]$ es una amplitud, definimos la longitud αl mediante la construcción siguiente:

1. Si $l = 0$ definimos $\alpha l = 0$.
2. Si $\alpha = 0, \pi$, definimos $\alpha l = l$.
3. Si no se dan los casos anteriores, sobre la semirrecta $\overrightarrow{bc}$ tomamos un punto c' tal que $\overline{bc'} \equiv \overline{uv}$. Esto es posible por el teorema sobre transporte de segmentos.
4. Al haber exceptuado los casos triviales, tenemos que $b \neq c'$ y que $bc \neq ba$, luego $c' \notin ba$ y podemos considerar el pie a' de la perpendicular a ba por el punto c'.

5. Definimos $\alpha l = [\overline{ba'}]$.



Técnicamente, la definición que hemos dado se puede plasmar en una fórmula $[\overline{pq}] = [\widehat{abc}][\overline{uv}]$ con siete variables libres que satisface las relaciones siguientes:

1. $a \neq b \neq c \rightarrow \bigvee pq\ [\overline{pq}] = [\widehat{abc}][\overline{uv}]$,

2. $\overline{uv} \equiv \overline{u^*v^*} \land \widehat{abc} \equiv \widehat{a^*b^*c^*} \land [\overline{pq}] = [\widehat{abc}][\overline{uv}] \land [\overline{p^*q^*}] = [\widehat{a^*b^*c^*}][\overline{u^*v^*}]$

$$\rightarrow \overline{pq} \equiv \overline{p^*q^*}.$$

En efecto, para probar la segunda propiedad en el caso no trivial usamos que, si además $\neg Rabc$, tenemos dos triángulos con hipotenusas iguales y dos ángulos iguales (el ángulo dado y un ángulo recto), luego son congruentes, por lo que sus catetos son congruentes. En el caso en que $Rabc$ es claro que $p = q$ y $p^* = q^*$.

Precisamente estas propiedades nos permiten hablar de αl sin necesidad de especificar los puntos que definen la amplitud o la longitud dada.

La interpretación es que αl representa lo que habitualmente representamos por $l|\cos\alpha|$.

Teorema 5.13 *Si $\alpha \neq \pi/2$ es una amplitud y l, l' son longitudes, entonces $\alpha l = \alpha l' \rightarrow l = l'$.*

Demostración: El resultado es trivial si $\alpha = 0$ o $\alpha = \pi$, por lo que podemos descartar ambos casos. Podemos expresar $\alpha = [\widehat{abc}]$ de modo que $[\overline{ac}] = l$ y, como por hipótesis bc no es la recta perpendicular a ba, el pie a' de la perpendicular a ba por c es un punto $a' \neq b$, con lo que tenemos un triángulo rectángulo $\widehat{a'bc}$ y además $[\overline{ba'}] = \alpha l$. Similarmente podemos tomar c' en $\overrightarrow{ac}$ tal que $[\overline{ac'}] = l'$, y el pie a'' de la perpendicular a ba por c' forma un triángulo rectángulo $\widehat{a''bc'}$ y $[\overline{ba''}] = \alpha l'$.

Por hipótesis, los triángulos $\widehat{a'bc}$ y $\widehat{a''bc'}$ tienen iguales dos ángulos (el de amplitud α y el ángulo recto) y un cateto de longitud $\alpha l = \alpha l'$, luego son congruentes y también tienen igual la hipotenusa, es decir, $l = l'$. ■

El resultado fundamental de esta trigonometría rudimentaria es el siguiente:

Teorema 5.14 *$\alpha\beta l = \beta\alpha l$.*

Demostración: Si alguno de los ángulos es $0, \pi/2, \pi$ el resultado es inmediato a partir de la definición, al igual que si $l = 0$. Así pues, supondremos que no se da ninguno de estos casos, lo que se traduce en que en la construcción de los productos se forman triángulos rectángulos no degenerados.

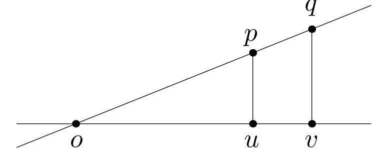
Concretamente, tenemos un triángulo rectángulo $Racb$ cuya hipotenusa $\overline{ab}$ tiene longitud l y cuyo cateto $\overline{ac}$ tiene longitud αl. A su vez, podemos construir el triángulo rectángulo $Radb$ con la misma hipotenusa y con un cateto $\overline{ad}$ de longitud βl, y por el teorema de traslación de triángulos podemos suponer que $c - ab - d$.

De este modo la situación es exactamente la del teorema 5.11. Consideramos el punto e dado por dicho teorema, el cual determina dos triángulos rectángulos. Concretamente, $[\widehat{cae}] = \beta$ y la hipotenusa es $[\overline{ac}] = \alpha l$, luego $[\overline{ae}] = \beta\alpha l$. Pero igualmente tenemos que $[\widehat{dae}] = \alpha$ y $[\overline{ad}] = \beta l$, luego $[\overline{ae}] = \alpha\beta l$. ■

Nos falta un último resultado previo elemental:

Teorema 5.15 $\mathrm{Col}(opq) \land \mathrm{Col}(ouv) \land u \neq o \neq v \land Rpuo \land Rqvo$

$$\to (p \sim_o q \leftrightarrow u \sim_o v).$$



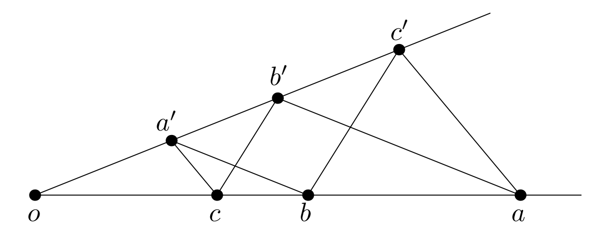
Si dos rectas cortan perpendicularmente a una recta en puntos u, v y a otra secante en puntos p, q, entonces p, q están al mismo lado del punto de corte o si y sólo si lo están u, v.

Demostración: Sea R la perpendicular a ou que pasa por o y que está contenida en el plano determinado por las dos rectas dadas. Como el pie de la perpendicular a ou por p es $u \neq 0$, tenemos que $pu \neq R$, luego $p \notin R$, e igualmente $q \notin R$. Además $R \parallel pu$ y $R \parallel qv$ porque tienen a uv como perpendicular común. Esto implica que $p \sim_R u \land q \sim_R v$, porque una recta no separa puntos de otra paralela. Por consiguiente, $p \sim_R q \leftrightarrow u \sim_R v$, lo cual a su vez equivale a que $p \sim_o q \leftrightarrow u \sim_o v$. ■

El teorema de Papos-Pascal es en realidad un teorema de la geometría proyectiva y, como suele suceder con tales teoremas, tiene traducciones distintas a la geometría afín que parecen muy diferentes entre sí, debido a que en geometría proyectiva no hay diferencia entre rectas paralelas y secantes. Aquí demostraremos dos variantes, y se podrían enunciar varias más.

En palabras, el teorema (en la versión que vamos a probar) afirma lo siguiente:

> *Consideremos dos rectas que se corten en un punto o, seleccionamos tres puntos a, b, c en una de ellas y otros tres a', b', c' en la otra (todos distintos de o); los unimos para formar un hexágono $ab'ca'c'a$. Si dos pares de lados opuestos (en el sentido de que serían opuestos si se tratara de un hexágono regular, es decir, un lado es opuesto al siguiente del siguiente del siguiente) son paralelos, digamos que $bc' \parallel cb' \land ca' \parallel ac'$, entonces el tercer par de lados opuestos también es paralelo: $ab' \parallel ba'$.*



Podemos dar una demostración que no dependa del axioma de las paralelas a cambio de usar una definición más fuerte de rectas paralelas:

Definición 5.16 Diremos que dos rectas son *paralelas respecto de un punto o* si

$$R \parallel_0 S \leftrightarrow \bigvee T \in \mathcal{R}(o \in T \land T \perp R \land T \perp S).$$

Es claro que, admitiendo el axioma de las paralelas, dos rectas coplanares R y S son paralelas si y sólo si cumplen $R \parallel_o S$ para cualquier punto o del plano que las contiene, ya que por o pasa una perpendicular a R en dicho plano, que será también perpendicular a S si y sólo si $R \parallel S$.

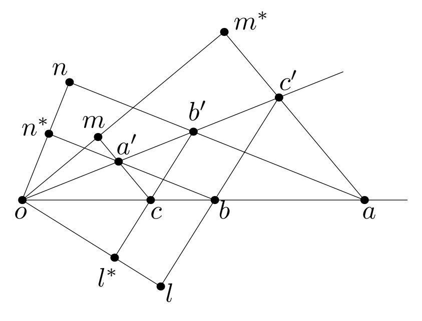
Teorema 5.17 (Teorema de Pappos-Pascal (versión absoluta))

$$\neg\mathrm{Col}(oaa') \land \mathrm{Col}(oabc) \land b \neq o \neq c \land \mathrm{Col}(oa'b'c') \land$$
$$b' \neq o \neq c' \land bc' \parallel_o cb' \land ca' \parallel_o ac' \rightarrow ab' \parallel_o ba'.$$

Por la observación precedente, si admitimos el axioma de las paralelas, este resultado equivale a:

Teorema 5.18 (Teorema de Pappos-Pascal (versión euclídea))

$$\neg\mathrm{Col}(oaa') \land \mathrm{Col}(oabc) \land b \neq o \neq c \land \mathrm{Col}(oa'b'c') \land$$
$$b' \neq o \neq c' \land bc' \parallel cb' \land ca' \parallel ac' \rightarrow ab' \parallel ba'.$$



Demostración: Por hipótesis existe una perpendicular común a bc' y a cb' que pasa por o. Llamemos l y l^* a los pies de dicha perpendicular en dichas rectas. Similarmente, existe una perpendicular común a ca' y ac' que pasa por o. Llamamos m y m^* a los pies correspondientes. Por último, tomamos una perpendicular a ab' por o y llamamos n a su pie en ab'. Definimos además las amplitudes siguientes:

$$\lambda = [\widehat{loc'}] = [\widehat{l^*ob'}], \quad \lambda' = [\widehat{lob}] = [\widehat{l^*oc}],$$
$$\mu = [\widehat{moa'}] = [\widehat{m^*oc'}], \quad \mu' = [\widehat{moc}] = [\widehat{m^*oa}]$$
$$\nu = [\widehat{noa}], \quad \nu' = [\widehat{nob'}].$$

Por otra parte, vamos a adoptar el convenio de representar con la misma letra cada punto $a, b, \ldots$ y la longitud correspondiente $[\overline{oa}], [\overline{ob}], \ldots$ Por la propia definición de producto de amplitud por longitud tenemos:

1. $\lambda' b = \lambda c' = l$,
2. $\mu' c = \mu a' = m$,
3. $\nu' a = \nu b' = n$,
4. $\lambda' c = \lambda b' = l^*$,
5. $\mu' a = \mu c' = m^*$,

   y vamos a demostrar:

6. $\nu' b = \nu a'$.

En efecto, usando repetidamente el teorema 5.14 obtenemos que

$$\lambda'\nu' b = \nu'\lambda' b =_1 \nu'\lambda c' \to \mu\lambda'\nu' b = \mu\nu'\lambda c' = \nu'\lambda\mu c' =_5 \nu'\lambda\mu' a$$

$$= \lambda\mu'\nu' a =_3 \lambda\mu'\nu b' = \mu'\nu\lambda b' =_4 \mu'\nu\lambda' c = \nu\lambda'\mu' c =_2 \nu\lambda'\mu a' = \mu\lambda'\nu a'.$$

Finalmente el teorema 5.13 nos da que $\nu' b = \nu a'$, como queríamos probar. Aquí hay que tener en cuenta que $\mu \neq \pi/2$, pues forma parte del triángulo rectángulo $Roma'$ salvo si $om = oa'$, en cuyo caso $\mu = 0$ o $\mu = \pi$, e igualmente se razona que $\lambda' \neq \pi/2$.

Llamemos n^* y n'^* a los pies de las perpendiculares a on que pasan por b y por a', respectivamente. Basta probar que $n^* = n'^*$, pues esto implica que $a'b$ es perpendicular a on, luego $ab' \parallel_o ba'$.

Por definición $\nu' b = n^* \wedge \nu a' = n'^*$, luego por 6) tenemos que $\overline{on'} \equiv \overline{on'^*}$. Por lo tanto, basta probar que $n^* \sim_o n \leftrightarrow n'^* \sim_o n$, pues entonces la unicidad del transporte de segmentos hace que $n^* = n'^*$.

A su vez, basta probar que $a \sim_o b \leftrightarrow a' \sim_o b'$, pues entonces, aplicando dos veces el teorema 5.15, tenemos:

$$n^* \sim_o n \leftrightarrow b \sim_o a \leftrightarrow a' \sim_o b' \leftrightarrow n'^* \sim_o n.$$

También por el teorema 5.15 vemos que

$$c \sim_o a \leftrightarrow m \sim_o m^* \leftrightarrow c' \sim_o a',$$

$$c \sim_o b \leftrightarrow l^* \sim_o l \leftrightarrow c' \sim_o b'.$$

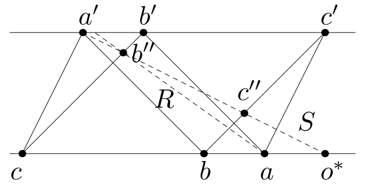
Como $(a \sim_o c \vee a{-}o{-}c) \wedge (b \sim_o c \vee b{-}o{-}c)$, podemos distinguir cuatro casos, y en los cuatro se cumple la condición que buscamos. Por ejemplo, si $a \sim_o c \wedge b \sim_o c$, por las equivalencias precedentes $a' \sim_o c' \wedge b' \sim_o c'$, luego $a \sim_o b \wedge a' \sim_o b'$. Si, por el contrario, $a \sim_o c \wedge b - o - c$, entonces $a' \sim_o c' \wedge b' - o - c'$, luego en este caso $a - o - b \wedge a' - o - b'$.

Igualmente, en los dos casos restantes llegamos a que los dos pares, a, b y a', b', están ambos al mismo lado de o o bien están ambos en lados opuestos de o. ■

La segunda versión del teorema de Pappos-Pascal que necesitamos es la correspondiente al caso en que las dos rectas dadas son paralelas en vez de secantes. En este caso es necesario el axioma de las paralelas:

Teorema 5.19 (Teorema de Pappos-Pascal (para rectas paralelas))

$$oa \parallel a'a' \land \mathrm{Col}(oabc) \land \mathrm{Col}(o'a'b'c') \land bc' \parallel cb' \land ca' \parallel ac' \to ab' \parallel ba'.$$



Demostración: Observemos en primer lugar que si dos de los puntos a, b, c son iguales la conclusión es trivial. Por ejemplo, si $a = b$ entonces tenemos que $cb' \parallel bc' = ac' \parallel ca'$, luego $a' = b'$, luego $ab' = ba'$. Si es $a = c$, entonces $ac' \parallel aa'$, luego $a' = c'$ y la hipótesis $bc' \parallel cb'$ equivale a la conclusión. Igualmente sucede si $b = c$, luego podemos suponer que los tres puntos a, b, c son distintos, y por simetría también que a', b', c' son distintos.

Sea R la paralela a $a'b$ que pasa por a. Tiene que cortar a cb', porque en caso contrario $a'b \parallel R \parallel cb' \parallel bc'$, luego $a' = c'$. Sea b'' el punto de corte de R con cb'. Basta probar que $b'' = b'$, pues entonces $R = ab'$. Supongamos lo contrario.

No puede ser $b'' = a'$, pues si $a' \in cb'$, entonces $a' = b'$. Sea $S = a'b'' \neq a'b'$. Como $cb' \parallel bc'$ y S corta a cb', también tiene que cortar a la recta bc' en un punto $c'' \neq c'$. Por el mismo motivo, S tiene que cortar a ab en un punto o^*.

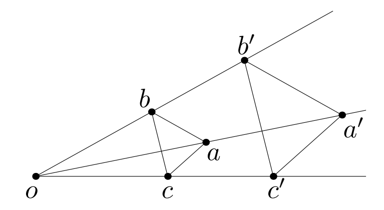
Sucede entonces que los puntos a, b, c, a', b'', c'' están en las hipótesis del teorema de Pappos-Pascal para rectas secantes. Concretamente, tenemos que $ba' \parallel ab'' \land cb'' \parallel c''b$, luego concluimos que $ca' \parallel ac''$, luego $ac'' \parallel ac'$, luego de hecho $ac'' = ac'$, y el punto de corte de esta recta con $bc' = bc''$ es $c' = c''$, contradicción. ■

5.3 El teorema de Desargues

Demostramos ahora el segundo teorema que necesitamos para dotar a las rectas de una estructura algebraica. La prueba requiere el axioma de las paralelas. El teorema de Desargues es también un teorema de la geometría proyectiva, por lo que tiene varias traducciones al caso afín. La versión básica es la siguiente:

Teorema 5.20 (Desargues)

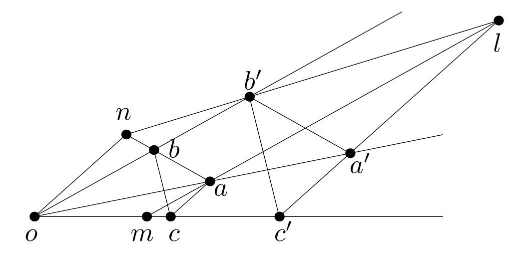
$$\neg\mathrm{Col}(abc) \land \mathrm{Cop}(abca') \land ab \parallel a'b' \land ab \neq a'b' \land ac \parallel a'c' \land ac \neq a'c' \land$$
$$\mathrm{Col}(oaa') \land \mathrm{Col}(obb') \land \mathrm{Col}(occ') \to bc \parallel b'c'.$$



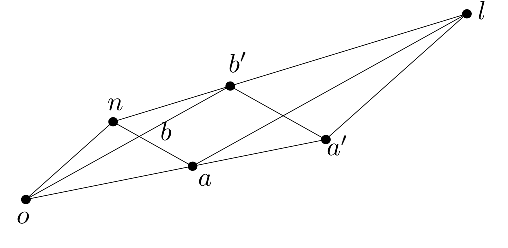
Si dos triángulos tienen sus vértices sobre rectas concurrentes coplanares, y dos pares de lados son paralelos, entonces los lados restantes también son paralelos.

Demostración: Se cumple que $o \notin ab$, pues en caso contrario la recta ab contendría también a b' y a su vez a a', luego $ab = a'b'$, en contra de lo supuesto. Igualmente se concluye que $o \notin ac$. Por otro lado, si $o \in bc$ concluimos igualmente que $bc = b'c'$, y la conclusión es inmediata. Por lo tanto podemos suponer también que $o \notin bc$. En definitiva, las rectas aa', bb', cc' son distintas dos a dos y su único punto en común es o. Distinguimos dos casos:

Caso 1 $\neg ob \parallel ac$.

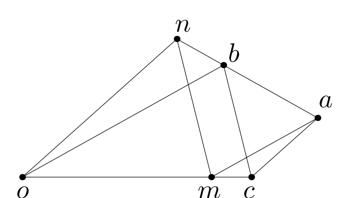


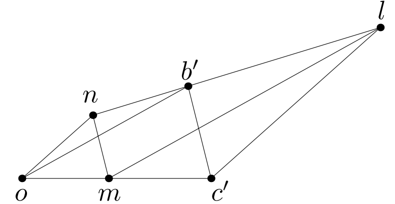
Entonces la paralela a ob por a no es ac, luego no es paralela a $a'c'$ (pues su única paralela por a es ac), luego la corta en un punto l. Sea m el punto de corte de al y oc (existe porque oc corta a ob, luego también a al, por ser paralela). Sea n el punto de corte de $b'l$ y ab. (Si no hubiera punto de corte significaría que $b'l$ sería la paralela a ab por b', pero ésta es $a'b'$, luego tendríamos que $l = a'$, pues ambos serían el punto de corte de $b'l = a'b'$ con $a'c'$, pero entonces $al = aa'$ no sería paralela a ob, contradicción.)



Podemos aplicar el teorema de Pappos-Pascal al hexágono indicado en la figura (tanto si las rectas que contienen a sus vértices son paralelas o secantes, pues tenemos probadas las dos versiones), y la conclusión es $on \parallel a'l = c'l = a'c'$. Por lo tanto, también $on \parallel ac$.

Aplicamos dos veces más el teorema de Pappos-Pascal a los hexágonos siguientes:

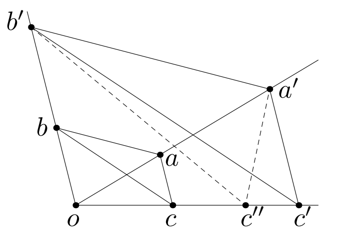




Del primero deducimos que $mn \parallel bc$ y del segundo que $mn \parallel b'c'$, luego en definitiva $bc \parallel b'c'$, como había que probar.

Caso 2 $ob \parallel ac$.

Por reducción al absurdo, supongamos que $\neg bc \parallel b'c'$. Entonces una de las dos rectas no es paralela a oa. Por la simetría de las hipótesis no perdemos generalidad si suponemos que es bc.



Consideramos la paralela a bc por b', que tiene que cortar a oc en un punto c'', porque oc corta a bc, luego también a sus paralelas. Además se cumple que $c'' \neq c'$, porque estamos suponiendo que $b'c'$ no es paralela a bc. Ahora los puntos $b - a - c - b' - a' - c''$ cumplen el caso 1 en lugar de $a - b - c - a' - b' - c'$, es decir, tenemos dos triángulos con vértices sobre rectas concurrentes, con dos pares de lados paralelos y oa no es paralela a bc. La conclusión es que $ac \parallel a'c''$, pero entonces $a'c' \parallel a'c''$ y $c' = c''$, contradicción. ■

Ahora probamos algunas variantes:

Teorema 5.21 (Desargues) *Supongamos* $\neg\mathrm{Col}(abc) \land \mathrm{Cop}(abca') \land ab \parallel a'b' \land ab \neq a'b' \land ac \parallel a'c' \land ac \neq a'c'$. *Entonces*

1. $bc \parallel b'c' \land bc \neq b'c' \land \mathrm{Col}(oaa') \land \mathrm{Col}(abb') \to \mathrm{Col}(acc')$,

2. $bc \parallel b'c' \land bc \neq b'c' \land aa' \parallel bb' \to cc' \parallel aa' \land cc' \parallel bb'$,

3. $aa' \parallel bb' \land aa' \parallel cc' \to bc \parallel b'c'$.

El apartado 1) es el recíproco del teorema anterior: Si suponemos que los lados de los triángulos son paralelos dos a dos y que dos pares de vértices están sobre rectas secantes, entonces el tercer par de vértices está sobre una recta concurrente con las otras dos.

El apartado 2) es lo mismo que 1), pero cambiando concurrentes por paralelas.

El apartado 3) es el análogo a la versión que hemos probado del teorema de Desargues, pero con rectas paralelas en vez de concurrentes.

Demostración: 1) La recta oc corta a bc, luego también a su paralela $b'c'$ en un punto c''. Entonces $a - b - c - a' - b' - c''$ están en las condiciones del teorema de Desargues ya demostrado: como $bc \parallel b'c''$ y $ba \parallel b'a'$, concluimos que $ac \parallel a'c''$, luego $a'c''$ es la paralela a ac por a', luego $a'c'' = a'c'$, luego $c'' = c'$, porque ambos son el punto de corte de esta recta con $b'c'$, luego $cc' = oc'$ pasa por o.

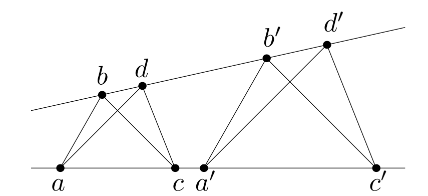
2) Si cc' no es paralela a aa', ambas rectas se cortan en un punto o, pero entonces estamos en las condiciones de 1), lo que implica que $\mathrm{Col}(obb')$, en contradicción con que $bb' \parallel aa'$.

3) Si bc no es paralela a $b'c'$ podemos considerar la paralela a bc por c', que cortará a bb' en un punto b'', pero entonces $a - b - c - a' - b'' - c'$ están en las condiciones de 2), luego $bb'' \parallel aa'$, luego bb'' es la paralela a cc' por b, luego es bb', luego $b' = b''$ y tenemos que bc sí que es paralela a $b'c'$, contradicción. ■

Veamos una consecuencia del teorema de Desargues que necesitaremos más adelante:

Teorema 5.22 $\mathrm{Cop}(R,S) \land a,c,a',c' \in R \setminus S \land b,d,b',d' \in S \setminus R \land$

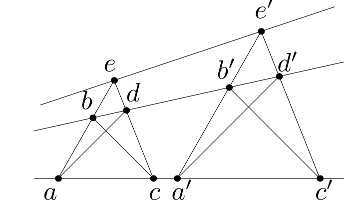
$$ab \parallel a'b' \land ad \parallel a'd' \land bc \parallel bc' \rightarrow cd \parallel c'd'.$$



DEMOSTRACIÓN: Si $b = d$, el paralelismo implica que $b' = d'$ y la conclusión es una de las hipótesis. Igualmente se razona si $a = c$, de modo que podemos suponer que los puntos a, b, c, d son distintos dos a dos. También podemos suponer que $a \neq a'$, pues en caso contrario concluimos que $d = d'$, $b = b'$, $c = c'$ y de nuevo la conclusión es trivial.

Supongamos que cd no es paralela a $c'd'$. Entonces una de las dos rectas no es paralela a ab, luego tampoco a $a'b'$. No perdemos generalidad si suponemos que es cd la que no es paralela. Llamemos e al punto de corte entre ab y cd.

Si R y S son secantes, sea T la recta que pasa por su punto de corte y por e. Si son paralelas, sea T la paralela a ambas que pasa por e. Como ab corta a T, también lo hace su paralela $a'b'$ en un punto e'.



Ahora aplicamos dos veces el teorema de Desargues (sea en la versión para rectas concurrentes o paralelas), primero a los triángulos $\widehat{aed}$ y $\widehat{a'e'd'}$, con lo que obtenemos que $ed \parallel e'd'$, y en segundo lugar a los triángulos $\widehat{bce}$ y $\widehat{b'c'e'}$, de donde concluimos que $ec \parallel e'c'$, pero $ec = ed$. Por lo tanto, $e'd'$ y $e'c'$ son ambas la paralela a ec por e', luego $e'c' = c'd'$ es paralela a $ec = cd$, contradicción. ■

5.4 La estructura de cuerpo

Imaginemos que quisiéramos demostrar el teorema de Tales, o el de Pitágoras (cosa que nos queda algo lejos). Para ello necesitaríamos definir primero la longitud de un segmento (para poder hablar de cuadrado de la hipotenusa, etc.) y eso se suele hacer por comparación con una unidad: fijado un segmento unidad, otro segmento tiene longitud p/q si es posible dividir el segmento unidad en q partes iguales y unir p de ellas hasta formar un segmento de la longitud del que queremos medir. Luego se ve que hay segmentos cuya longitud no puede expresarse de este modo respecto a la longitud del segmento unitario, pero los números racionales r tales que los segmentos de longitud r son menores que el segmento dado forman una sección inicial de $\mathbb{Q}$ que determina un número real $\mathbb{R}$, y dicho número real se toma como definición de la longitud del segmento.

En la geometría de Tarski no podemos asociar un número real a cada segmento, porque no podemos definir el concepto de número real, pero sí que podemos definir geométricamente una suma y un producto sobre los puntos de la recta, de modo que los propios puntos puedan representar el papel de números y tenga sentido hablar del cuadrado de la hipotenusa en el teorema de Pitágoras, o de las razones entre los lados de un triángulo en el teorema de Tales.

5.4.1 La suma geométrica

Empezamos definiendo la suma geométrica en una recta. Para ello conviene introducir algunas nociones auxiliares. Por ejemplo, diremos que unos puntos $a_1, \ldots, a_n$ están en *posición aritmética* respecto de unos puntos o y e si se cumple

$$\mathrm{Ar}_{oe} a_1, \ldots, a_n \leftrightarrow o \neq e \land \mathrm{Col}(o, e, a_1, \ldots, a_n),$$

es decir, si o y e son puntos distintos y todos los demás están sobre la recta que determinan. Diremos que los puntos están en posición aritmética respecto a o y e *con punto auxiliar* e' si

$$\mathrm{Ar}^{e'}_{oe} a_1, \ldots, a_n \leftrightarrow \neg\mathrm{Col}(oee') \land \mathrm{Col}(o, e, a_1, \ldots, a_n),$$

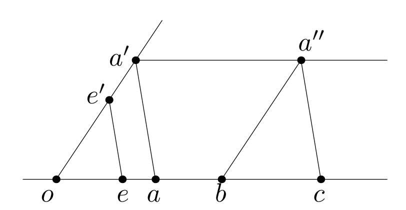
lo que supone exigir que o, e, e' no sean colineales, y en particular que sean distintos dos a dos. Además escribiremos:

$$\mathrm{Par}(abcd) \leftrightarrow a \neq b \land (c \neq d \rightarrow ab \parallel cd).$$

Esto significa que a y b son distintos y que d está en la paralela a ab que pasa por c.

Ahora podemos definir la *suma* de dos puntos respecto de tres puntos dados o, e, e':

$$\mathrm{Suma}^{e'}_{oe}(abc) \leftrightarrow \mathrm{Ar}^{e'}_{oe} abc \land$$
$$\bigvee a'a''(\mathrm{Par}(ee'aa') \land \mathrm{Col}(oe'a') \land \mathrm{Par}(oea'a'') \land \mathrm{Par}(oe'ba'') \land \mathrm{Par}(ee'a''c)).$$



Más detalladamente, tenemos una recta R en la cual hemos seleccionado un origen o, una unidad e y aparte un punto auxiliar e' fuera de R. Tomamos dos puntos $a, b \in R$ y definimos su suma (respecto a o, e, e') como el punto de R construido de este modo:

1. Trazamos la paralela a ee' que pasa por a y consideramos el punto a' en el que corta a oe'. Dicho punto existe porque oe' corta a ee', luego también a sus paralelas. Si $a = o$, entonces $a' = o$ por definición y si $a = e$ entonces $a' = e'$.

2. Trazamos la paralela a oe por a' y la paralela a oe' por b. Ambas rectas se cortan en un punto a'' porque la segunda recta corta a oe, luego también a sus paralelas. Si $a = o$ entonces $a' = o$, la primera recta es la propia $R = oe$ y $a'' = b$ por definición.

3. Trazamos la paralela a oe por a'' y llamamos c (la suma) al punto donde corta a R (que será el propio b si $a = o$).

Es claro que esta construcción determina un único punto c, es decir, que cumple

$$\mathrm{Ar}_{oe}^{e'}ab \rightarrow \overset{1}{\bigvee} c\ \mathrm{Suma}_{oe}^{e'}(abc).$$

Usaremos la notación $c = a + b$ cuando no sea necesario especificar los puntos o, e, e' con los que se calcula la suma.

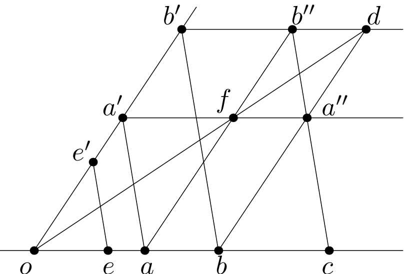
Hemos demostrado que $o + b = b$. También es claro que $a + o = a$, pues en este caso, una vez hemos obtenido el punto a', la paralela a oe' que pasa por $b = 0$ es oe', luego $a'' = a'$, la paralela a oe' que pasa por $a'' = a'$ es de nuevo aa', luego $c = a$.

Así pues, la suma que acabamos de definir tiene a o por elemento neutro. Otra propiedad elemental es que $a + b = a + b^* \rightarrow b = b^*$, pues si $b \neq b^*$, entonces las paralelas a oe' por b y b^* serán rectas distintas que cortarán a la paralela a oe por a' en dos puntos distintos a'' y $(a'')^*$, luego las paralelas a ee' por estos puntos serán dos rectas distintas que cortarán a oe en dos puntos distintos $a + b \neq a + b^*$.

Veamos que la suma es conmutativa:

Teorema 5.23 $\mathrm{Ar}_{oe}^{e'}ab \rightarrow a + b = b + a.$

Demostración: Lo tenemos probado ya si $a = o$ o $b = o$, y es trivial si $a = b$, luego podemos descartar estos casos.



La figura siguiente muestra la construcción de $a+b$ y de $b+a$. Observemos que $a \neq b$ implica que $a' \neq b'$, luego las paralelas $a'a''$ y $b'b''$ son distintas, luego $a'' \neq b''$. El punto c se obtiene, por una parte, como el corte con oe de la paralela a ee' que pasa por a'' y, por otra parte, como el corte con oe de la paralela a ee' que pasa por b''. Para probar que se trata del mismo punto en ambos casos basta demostrar que $a''b'' \parallel ee'$, pues así la paralela a ee' por a'' es la misma que la paralela a ee' por b''.

Para ello llamamos d al corte entre ba'' y $b'b''$ (que existe, porque ba'' corta a $a'a''$, que, por construcción, es paralela a oe, luego a $b'b''$, y si una recta corta a otra, corta a todas sus paralelas). Igualmente podemos considerar el punto f donde ab'' corta a $a'a''$.

Ahora aplicamos el recíproco del teorema de Desargues a los triángulos $\widehat{aa'f}$ y $\widehat{bb'd}$. Por construcción tienen sus lados paralelos dos a dos, y las rectas $a'b'$ y ab se cortan en o, luego concluimos que fd también pasa por o.

A continuación aplicamos el teorema de Desargues a los triángulos $\widehat{b'bo}$ y $\widehat{b''a''f}$. Las rectas $b'b''$, ba'' y of se cortan en d y los triángulos tienen dos pares de lados paralelos. Concluimos que el tercer par también es paralelo, es decir, que $bb' \parallel a''b''$, luego $a''b'' \parallel aa'$. ■

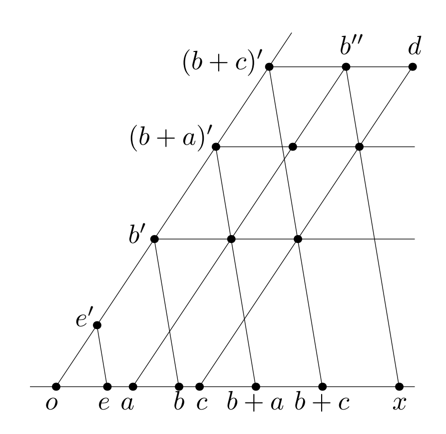
Ahora demostramos la asociatividad:

Teorema 5.24 $\mathrm{Ar}_{oe}^{e'}abc \rightarrow a + (b + c) = (a + b) + c.$

Demostración: Como ya hemos probado la conmutatividad, es equivalente probar que $(b + a) + c = (b + c) + a$.

Si alguno de los puntos es o la conclusión se sigue de la conmutatividad ya demostrada. Lo mismo vale en el caso $a = c$, luego podemos suponer que $a \neq c$, luego $b + a \neq b + c$. Además ambos son distintos de b, o de lo contrario $a = o$ o bien $b = o$, porque ya hemos probado que la suma es simplificable.

La figura muestra la construcción de $(b+a)+c$ y de $(b+c)+a$. En ambos casos obtenemos el punto x, y para probar que esto no es casual, tenemos que demostrar que $b''a'' \parallel ee'$.



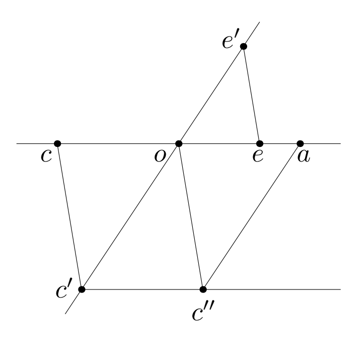
Ahora bien, la parte de la figura por encima de la horizontal que pasa por b' es idéntica a la figura de la prueba del teorema 5.23 con exactamente las mismas hipótesis (con b' en lugar de o), luego aplicando exactamente igual el teorema de Desargues llegamos a que

$$b''a'' \parallel (b + a)'(b + a),$$

luego $b''a'' \parallel ee'$. ■

Teorema 5.25 $\mathrm{Ar}_{oe}^{e'}a \rightarrow \overset{1}{\bigvee} c\ c + a = o.$

Demostración: La unicidad es inmediata porque ya hemos probado que la suma es simplificable: si $c+a = o = c'+a$, entonces $c = c'$. Para probar la existencia de c podemos suponer que $a \neq o$, pues para $a = 0$ sirve $c = 0$.



Basta tomar $c = S_o a$. La figura muestra la construcción de $c + a$. Trazamos la paralela a ee' por c y la cortamos con oe' en c', luego trazamos la paralela a oe por c' y la cortamos

con la paralela a oe' por a en c''. Finalmente trazamos la paralela a ee' por c'', y tenemos que probar que pasa por o.

Para ello observamos que $c - oc' - a$ y que $a \sim_{oc} c''$, porque la recta ac'' es paralela a oc', luego ésta no puede separar puntos de aquélla. Por lo tanto $c - oc' - c''$, y así podemos aplicar el teorema 5.6 4):

$$oc \parallel c'c'' \wedge \overline{oc} \equiv \overline{c'c''} \wedge c - oc' - c'' \to oc'' \parallel cc',$$

luego oc'' es la recta paralela a ee' que pasa por c''. ■

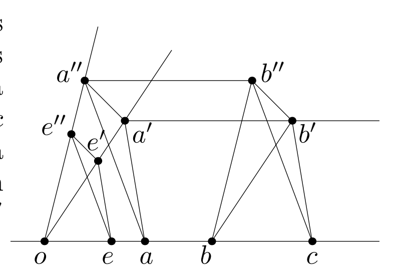
Con esto hemos dotado a cada recta de estructura de grupo.

Teorema 5.26 *La suma en una recta no depende de la elección de e'.*

DEMOSTRACIÓN: Tomamos otro punto e'' tal que $\neg\text{Col}(oee'')$ y vamos a probar que $a + b$ es el mismo tanto si lo calculamos con e' como con e''. Si $a = o$ o $b = o$ es inmediato, así que suponemos lo contrario. También podemos suponer que $e' \neq e''$. Distinguimos dos casos:

Caso 1 o, e, e', e'' son coplanares.

La figura muestra la construcción de las dos sumas. Podemos suponer que $a' \neq a''$, pues en caso contrario $b' = b''$ y la suma c es la misma en las dos construcciones. Llamamos c al punto donde la paralela a ee' por b' corta a oe, y tenemos que probar que coincide con el punto de corte de oe con la paralela a ee'' por b''. Distinguimos dos subcasos:



Caso 1a $\neg a'a'' \parallel oe$.

Esto implica que las paralelas a oe por a' y a'' son distintas, que es el caso que muestra la figura. Podemos aplicar la versión del teorema de Desargues para rectas paralelas a los triángulos $\widehat{oa'a''}$ y $\widehat{bb'b''}$ para concluir que $a'a'' \parallel b'b''$. (No podemos aplicarlo si $\text{Col}(oa'a'')$, pero eso equivale a $\text{Col}(oe'e'')$, y entonces la paralela a oe' por b es la misma que la paralela a oe'' por b, luego también son colineales b, b', b'' y también concluimos que $a'a'' \parallel b'b''$.)

Ahora aplicamos el teorema de Desargues a los triángulos $\widehat{aa'a''}$ y $\widehat{cb'b''}$ para concluir que $b''c \parallel a''a$, luego $b''c$ es la paralela a ee'' por b'', como había que probar.

Caso 1b $a'a'' \parallel oe$.

En este caso $a'a'' = b'b''$ y podemos aplicar el teorema 5.22.

Caso 2 o, e, e', e'' no son coplanares. (Este caso lo ilustra igualmente la figura, imaginándola tridimensional.)

En este caso las rectas oa', oa'', ab', ob'' cumplen el teorema 5.9 3), por lo que los planos $P_1 = oaa'$ y $P_2 = bb'b''$ son paralelos.

Por otra parte, las rectas $a'b'$ y $a''b''$ son paralelas (pues ambas son paralelas a ab) y el plano P que las contiene corta a P_1 y P_2 en $a'a''$ y $b'b''$. El teorema 5.9 2) implica que estas rectas son paralelas. Por la parte 3) de dicho teorema, aplicada a las rectas $aa', a'a'', cb', b'b''$, obtenemos que los planos $Q_1 = aa'a''$ y $Q_2 = cb'b''$ son paralelos, luego el plano Q que contiene a las paralelas ac y $a''b''$ corta a estos planos en las rectas paralelas aa'' y cb'', luego cb'' es la paralela a ee'' por b'', luego ésta corta a oe en c. ■

Como consecuencia:

Teorema 5.27 *La suma en una recta tampoco depende de la elección de* e.

Demostración: Consideramos tres puntos o, e, e^* colineales distintos dos a dos. Fijemos un punto e' no colineal con ellos y sea e'^* el punto en que la paralela a ee' por e^* corta a oe'.

Ahora basta observar que en la definición de suma los puntos e y e' sólo se usan para determinar paralelas respecto de la recta ee', por lo que la suma definida con e y e' es la misma que la definida con e^* y e'^*, pues las paralelas de ee' son las mismas que las de $e^*e'^*$, y esta suma a su vez es la misma que la definida con e^* y e', por el teorema anterior. ■

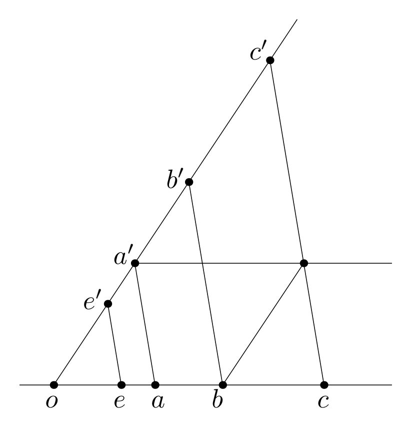
Obviamente, la suma sí que depende de la elección de o, pues éste es el elemento neutro respecto de la suma que determina.

Terminamos con un resultado que necesitaremos después:

Teorema 5.28 $c = (a+b)_{oe}^{e'} \wedge \mathrm{Ar}_{oe'}(a'b'c') \wedge \mathrm{Par}(ee'aa') \wedge \mathrm{Par}(ee'bb')$

$$\rightarrow c' = (a'+b')_{oe'}^{e}.$$

Esto significa que la proyección paralela de la recta oe en la recta oe', es decir, la aplicación que a cada punto a le asigna el punto a' donde la paralela a ee' por a corta a oe' es un isomorfismo de grupos.

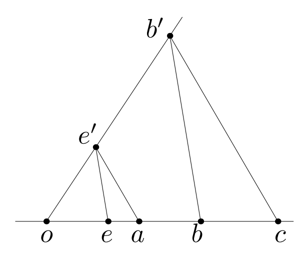


Demostración: Sin más que aplicar las definiciones se comprueba trivialmente que si $c = (a+b)_{oe}^{e'}$, entonces $c' = (b'+a')_{oe'}^{e}$. ■

5.4.2 El producto geométrico

Definimos ahora un *producto* en una recta respecto a un origen o, una unidad e y un punto auxiliar e':

$$\mathrm{Prod}_{oe}^{e'} \leftrightarrow \mathrm{Ar}_{oe}^{e'}abc \land \bigvee b'(\mathrm{Par}(ee'bb') \land \mathrm{Col}(oe'b) \land \mathrm{Par}(e'ab'c)).$$



En palabras, la construcción del producto de los puntos a y b se realiza como sigue:

1) Trazamos la paralela a ee' por b y consideramos el punto b' donde corta a oe' (si $b = o$ será $b' = o$).

2) Trazamos la paralela a ae' por b', y el producto es el punto c donde ésta corta a oe (que será o si $b = b' = o$).

Si consideramos que oe tiene longitud 1, el teorema de tales implica que

$$\frac{\overline{oc}}{\overline{oa}} = \frac{\overline{ob'}}{\overline{oe'}} = \frac{\overline{ob}}{\overline{oe}} = \overline{ob},$$

luego la longitud de $\overline{oc}$ es el producto de las longitudes de $\overline{oa}$ y $\overline{ob}$. Pero no tenemos demostrado el teorema de Tales (ni siquiera tiene sentido hablar en nuestro contexto de la longitud de un segmento, considerada como un número), por lo que esta "demostración" no tiene sentido en este momento. Lo que hacemos es tomar esta consecuencia del teorema de Tales como definición de producto y más adelante estaremos en condiciones de deducir de ella el teorema de Tales.

Es claro que la construcción que hemos descrito determina un único punto c para cada par de puntos a y b en la recta oe, por lo que podemos escribir $c = ab$ cuando no sea necesario especificar los puntos o, e, e' respecto a los que se realiza la construcción.

Ya hemos observado que $a \cdot o = o$, y también es trivial que $o \cdot a = o$, porque en este caso la paralela a $ae' = oe'$ que pasa por b' es oe' y corta a oe en $c = o$.

También es inmediato que $ae = ea = a$. Por ejemplo, si $b = e$, la paralela a ee' por $b = e$ es ee', que corta a oe' en $b' = e'$, luego la paralela a ae' por b' es ae', y corta a oe en $c = a$.

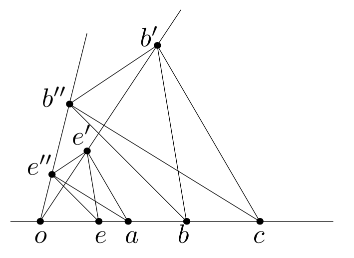
En particular vemos que, a diferencia de lo que sucedía con la suma, el producto sí que depende de la elección de e, pues éste actúa como elemento neutro.

Teorema 5.29 *El producto geométrico no depende de la elección del punto auxiliar e'.*

DEMOSTRACIÓN: Consideramos otro punto e'' tal que $\neg\mathrm{Col}(oee'')$. Podemos suponer que $e' \neq e''$. Distinguimos dos casos:

Caso 1 o, e, e', e'' son coplanares.

La figura muestra la construcción del producto de dos puntos a y b respecto de ambos puntos auxiliares. Llamamos c al producto construido con e' y vamos a probar que es también el construido con e''. Esto equivale a probar que la paralela a ae'' por b'' es $b''c$. Distinguimos dos subcasos:



Caso 1a $\neg\mathrm{Col}(oe'e'')$.

Aplicamos el teorema de Desargues a los triángulos $\widehat{ee'e''}$ y $\widehat{bb'b''}$, que tienen dos pares de lados paralelos, luego también $e'e'' \parallel b'b''$. A su vez, esto nos permite aplicar el mismo teorema a los triángulos $\widehat{ae'e''}$ y $\widehat{cb'b''}$, que también tienen dos pares de lados paralelos, luego $b''c \parallel ae''$, como había que probar.

Caso 1b $\mathrm{Col}(oe'e'')$.

Entonces $oe' = oe''$ y basta aplicar el teorema 5.22.

Caso 2 o, e, e', e'' no son coplanares. (Este caso lo ilustra igualmente la figura, imaginándola tridimensional.)

Como las rectas ee' y ee'' son paralelas a bb' y bb'', respectivamente, el teorema 5.9 implica que los planos $ee'e''$ y $bb'b''$ son paralelos, y como el plano $oe'e''$ corta a dichos planos en las rectas $e'e''$ y $b'b''$, el mismo teorema implica que $e'e'' \parallel b'b''$.

A su vez, las rectas $e'a$ y $e'e''$ son paralelas a $b'c$ y $b'b''$, respectivamente, luego los planos $ae'e''$ y $cb'b''$ son paralelos, y el plano oee'' los corta en las rectas ae'' y cb'', luego éstas son paralelas. ■

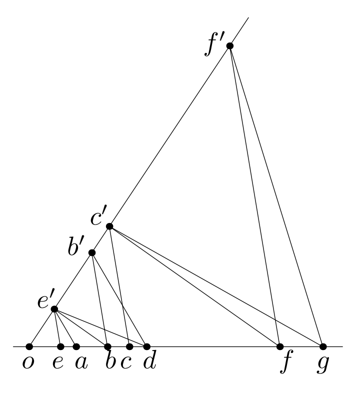
Veamos la asociatividad del producto:

Teorema 5.30 $\mathrm{Ar}_{oe}^{e'}abd \rightarrow (ab)c = a(bc)$.

DEMOSTRACIÓN: Suponemos $b \neq o$, pues en otro caso la conclusión es trivial. Llamaremos $d = ab$, $f = bc$ y $g = dc$, de modo que lo que hay que probar es que $af = g$.

La figura muestra la construcción de estos puntos. Hay que probar que la paralela a ae' por f' pase por g, es decir, que $f'g \parallel ae'$.

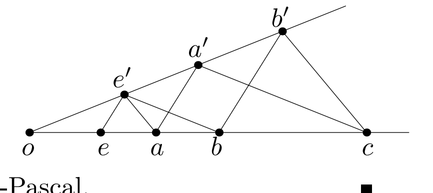
Es inmediato comprobar por la propia definición que $\mathrm{Prod}_{ob}^{e'}(dfg)$, luego también se cumple $\mathrm{Prod}_{ob}^{b'}(dfg)$, porque hemos visto que el producto no depende de la elección del punto auxiliar, y esto implica que $f'g \parallel b'd \parallel ae'$. ■



La conmutatividad del producto es el teorema de Pappos-Pascal:

Teorema 5.31 $\mathrm{Ar}_{oe}^{e'}ab \rightarrow ab = ba$.

DEMOSTRACIÓN: Podemos suponer que $a \neq o \neq b$. La figura muestra la construcción de $c = ab$. Para que se cumple $c = ba$ sólo hace falta que la paralela a be' por a' pase por c, es decir, que $a'c \parallel be'$, pero eso es justo lo que afirma el teorema de Pappos-Pascal. ■



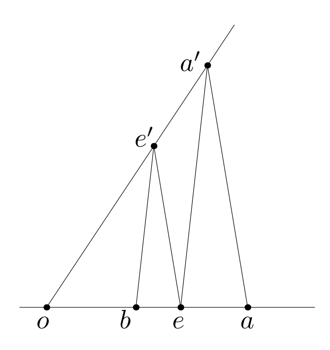
La existencia de inversos es fácil de probar:

Teorema 5.32 $\mathrm{Ar}_{oe}^{e'}a \wedge a \neq o \rightarrow \stackrel{1}{\bigvee} b\, ba = e$

DEMOSTRACIÓN: Trazamos la paralela a ee' que pasa por a, la cual cortará a oe' en un punto $a' \neq o$. Luego trazamos la paralela a ea' por e', que cortará a oe en un punto b. Se comprueba inmediatamente que $ba = e$.

La unicidad es consecuencia de un argumento algebraico general: si b' es otro inverso de a

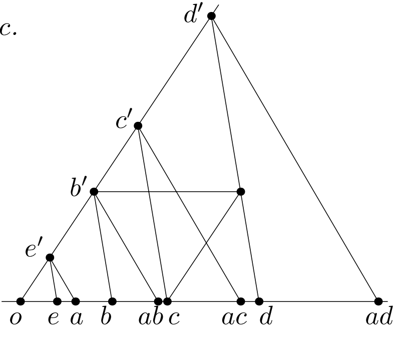
$$b' = b'e = b'ab = eb = b.$$ ■



Por último probamos la propiedad distributiva:

Teorema 5.33 $\mathrm{Ar}_{oe}^{e'}abc \rightarrow a(b + c) = ab + ac$.

DEMOSTRACIÓN: Podemos suponer que $b \neq o$. Llamemos $d = b + c$. El teorema 5.28 nos da que $d' = (b' + c')_{oe'}^{e}$. Como la suma no depende del punto auxiliar, $d' = (b' + c')_{oe'}^{a}$. De nuevo por el teorema 5.28 obtenemos que $d'' = (b'' + c'')_{oa}^{e'}$, donde las dobles primas indican la proyección paralela a $e'a$, pero por definición resulta que $b'' = ab$, $c'' = ac$ y $d'' = ad$. Como la suma tampoco depende del punto unidad, $d'' = (b'' + c'')_{oe}^{e'}$, es decir, $ad = ab + ac$. ■



Con esto tenemos probado que cada par de puntos distintos o, e determinan una estructura de cuerpo en la recta oe, de modo que se cumplen los axiomas de la teoría C interpretando las constantes $0, 1$ como o y e, respectivamente.

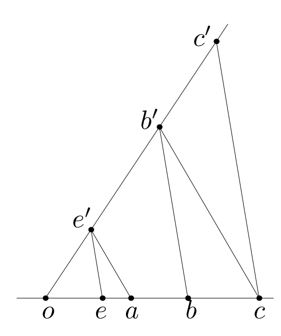
5.4.3 Isomorfismos de cuerpos

Hemos probado que en cada recta podemos definir infinitas estructuras de cuerpo, según la elección de los puntos o y e. Ahora demostraremos que todos los cuerpos obtenidos de esta forma en distintas rectas mediante la elección de distintos pares de puntos o y e son isomorfos. Empezamos extendiendo el teorema 5.28 para abarcar también el producto:

Teorema 5.34 $\mathrm{Prod}_{oe}^{e'}(abc) \wedge \mathrm{Ar}_{oe'}a'b'c' \wedge \mathrm{Par}(ee'aa') \wedge \mathrm{Par}(ee'bb') \wedge \mathrm{Par}(ee'cc')$

$$\rightarrow \mathrm{Prod}_{oe'}^{e}(a'b'c').$$

Esto, junto con 5.28, quiere decir que la proyección de oe en oe' paralela a ee' es un isomorfismo de cuerpos.



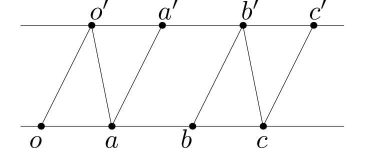
DEMOSTRACIÓN: Podemos suponer que $a \neq o$, y entonces es inmediato comprobar a partir de la definición que $\mathrm{Prod}_{oe}^{e'}(abc)$ implica $\mathrm{Prod}_{oe'}^{a}(a'b'c')$, que es equivalente a $\mathrm{Prod}_{oe'}^{e}(a'b'c')$ porque hemos visto que el producto no depende de la elección del punto auxiliar. ■

Seguidamente demostramos que la proyección paralela entre rectas paralelas también es un isomorfismo de cuerpos:

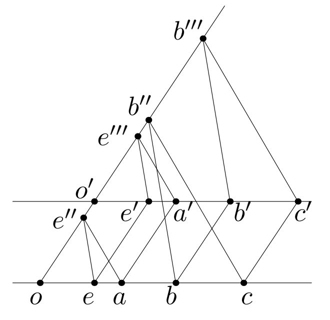
Teorema 5.35 $oe \parallel o'e' \wedge oe \neq o'e' \wedge \mathrm{Ar}_{oe}abc \wedge \mathrm{Ar}_{o'e'}a'b'c' \wedge$

$$\mathrm{Par}(oo'aa') \wedge \mathrm{Par}(oo'bb') \wedge \mathrm{Par}(oo'cc') \rightarrow$$

$$(\mathrm{Suma}_{oe}^{e'}(abc) \rightarrow \mathrm{Suma}_{o'e'}^{e}(a'b'c')) \wedge (\mathrm{Prod}_{oe}^{e'}(abc) \rightarrow \mathrm{Prod}_{o'e'}^{e}(a'b'c')).$$



DEMOSTRACIÓN: En primer lugar probamos que la proyección conserva la suma. Podemos suponer que $a \neq o$. Si se cumple $\mathrm{Suma}_{oe}^{e'}(abc)$, entonces $\mathrm{Suma}_{oa}^{o'}(abc)$, porque la suma no depende ni de e ni de e'. Y de la propia definición de suma se sigue inmediatamente que esto equivale a $\mathrm{Suma}_{o'e'}^{a}(a'b'c')$, que a su vez equivale a $\mathrm{Suma}_{o'e'}^{e}(a'b'c')$.



El caso del producto es algo más delicado. Podemos suponer que $a, b, c \neq o$. Sea e'' un punto en la recta oo' distinto de o. Como el producto no depende del punto auxiliar, tenemos $\mathrm{Prod}_{oe}^{e''}(abc)$. Llamemos e''' al punto dado por $\mathrm{Suma}_{oe''}^{e}(e''oe''')$. Por construcción $e'''e' \parallel ee''$.

Por la independencia de la suma respecto del punto auxiliar, también $\mathrm{Suma}_{oe''}^{a}(e'', o', e''')$, lo que en particular implica que $a'e''' \parallel ae''$.

Ahora construimos b''' mediante $\mathrm{Suma}_{ob''}^{b'}(b''o'b''')$, con lo que también se cumplirá $\mathrm{Suma}_{ob''}^{c}(b''o'b''')$. Esto implica que $b'b''' \parallel b''b$, y también $c'b''' \parallel cb''$.

Es claro entonces que se cumple $\mathrm{Prod}_{o'e'}^{e'''}(a'b'c')$, luego $\mathrm{Prod}_{o'e'}^{e}(a'b'c')$. ■

Así pues, hemos encontrado dos tipos del isomorfismos de cuerpos entre rectas:

1. Los *isomorfismos de tipo* 1, que son las proyecciones paralelas de una recta oe en otra oe' mediante paralelas a ee'.
2. Los *isomorfismos de tipo* 2, que son las proyecciones paralelas de una recta oe en otra paralela distinta $o'e'$ con la condición de que $oo' \parallel ee'$, y la proyección se realiza mediante rectas paralelas a éstas.

Ahora es fácil concluir en general:

Teorema 5.36 *Todos los pares o, e de puntos distintos determinan cuerpos isomorfos, de modo que un isomorfismo entre dos de ellos puede obtenerse componiendo como máximo tres isomorfismos de los dos tipos que acabamos de describir.*

DEMOSTRACIÓN: Consideremos dos pares de puntos o, e y o', e' y distingamos varios casos:

Caso 1 $o = o'$.

Si $\neg\mathrm{Col}(oee')$ basta un isomorfismo de tipo 1. Si $\mathrm{Col}(oee')$, tomamos otro punto e'' no colineal y componemos el isomorfismo entre oe y oe'' con el isomorfismo entre oe'' y oe'.

Caso 2 $o \neq o'$. Distinguimos varios subcasos:

Caso 2a $o' \notin oe$.

Si $oe \parallel o'e'$, basta un isomorfismo de tipo 2, mientras que si ambas rectas son secantes tomamos la paralela a oe por o', que será de la forma $o'e''$, y componemos el isomorfismo de tipo 2 de oe en $o'e''$ con el isomorfismo de tipo 1 de $o'e''$ en $o'e'$.

Caso 2b Si $o' \notin o'e'$ razonamos análogamente.

Caso 2c Si no se dan los dos subcasos anteriores, tenemos $o' \in oe \land o \in o'e'$, con lo que $oe = oo' = o'e'$. Entonces tomamos una recta secante oe'' y su paralela por o', y tomamos el punto e''' donde ésta corta a la paralela de oe por e'' (con lo que formamos un paralelogramo de vértices o, o', e'', e''').

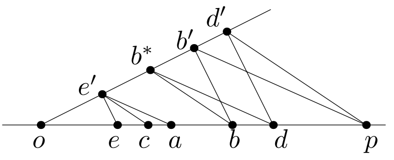
En este caso componemos tres isomorfismos: de de oe en oe'', de tipo 1, el de oe'' en $o'e'''$, de tipo 2, y el de $o'e'''$ en $o'e'$, de tipo 1. ■

Probamos ahora un resultado técnico:

Teorema 5.37 $\mathrm{Ar}_{oe}^{e'}abcd \land c \neq o \rightarrow (ab = cd \leftrightarrow \mathrm{Prod}_{oc}^{e'}(abd))$.

(Aquí ab y cd son los productos respecto de o y e.)

DEMOSTRACIÓN: Podemos suponer que $a, b, d \neq o$. Para probar una implicación partimos de que $ab = cd = p$. La figura muestra la situación.



Para construir el producto $(ab)^{e'}_{oc}$ levantamos b paralelamente a ce', con lo que llegamos a b^* y luego tenemos que construir la paralela a ae' por b^*, y se trata de probar que es b^*d. Ahora bien, esto es consecuencia inmediata del teorema de Pappos-Pascal aplicado al hexágono que muestra la figura.

Para probar el recíproco suponemos $\mathrm{Prod}^{e'}_{oc}(abd)$ y tomamos el punto d_0 que cumple $ab = cd_0$. Esto es posible porque estamos en un cuerpo y $c \neq 0$. Por la implicación ya probada se cumple $\mathrm{Prod}^{e'}_{oc}(abd_0)$ y, como el producto de dos puntos es único, tiene que ser $d = d_0$, luego $ab = dc$. ■

Como consecuencia tenemos lo siguiente:

Teorema 5.38 $\mathrm{Ar}^{e'}_{oe}abcd \land \mathrm{Col}(oeu) \land u \neq o \land (ab)^{e'}_{oe} = (cd)^{e'}_{oe} \rightarrow (ab)^{e'}_{ou} = (cd)^{e'}_{ou}$.

Esto significa que, aunque el producto depende de la elección de e, una relación de la forma $ab = cd$ se sigue cumpliendo si cambiamos la unidad e por otra u (necesariamente en la misma recta). Aunque sea un caso ligeramente más particular, el significado de este hecho se entiende mejor si escribimos la igualdad como $a/c = d/b$ (aunque entonces hay que exigir que $c \neq o \neq b$). Lo que dice el teorema es que el hecho de que dos pares de números sean proporcionales es independiente de la elección de la unidad.

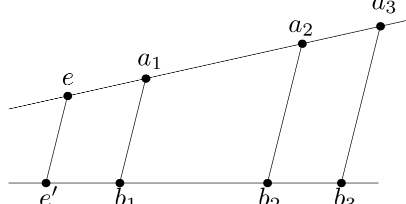
Demostración: Llamemos p y q a los productos $\mathrm{Prod}^{e'}_{ou}(abp)$, $\mathrm{Prod}^{e'}_{ou}(cdq)$. El teorema anterior afirma que $ab = up \land cd = uq$ (donde los productos se calculan mediante e), luego $ab = cd \leftrightarrow up = uq \leftrightarrow p = q$. ■

5.4.4 La ordenación de las rectas

Ahora demostraremos que las rectas pueden dotarse de una relación de orden compatible con la estructura de cuerpo. Para ello demostramos primero un resultado elemental:

Teorema 5.39 *Sean R y R' dos rectas y consideremos puntos $e \in R \setminus R'$, $e' \in R' \setminus R$, $a_1, a_2, a_3 \in R$, $b_1, b_2, b_3 \in R'$, de modo que* $\mathrm{Par}(ee'a_1b_1)$, $\mathrm{Par}(ee'a_2b_2)$, $\mathrm{Par}(ee'a_3b_3)$. *Entonces*

$$a_1 - a_2 - a_3 \leftrightarrow b_1 - b_2 - b_3, \qquad a_2 \sim_{a_1} a_3 \leftrightarrow b_2 \sim_{b_1} b_3.$$



Se trata de probar que las proyecciones paralelas entre rectas conservan las relaciones “estar en lados opuestos” y “estar al mismo lado”.

Demostración: Podemos suponer que los tres puntos a_1, a_2, a_3 son distintos dos a dos, pues si dos de ellos coinciden sus imágenes coinciden también, y el resultado se vuelve trivial. Llamamos $T = a_2b_2$ si $a_2 \neq b_2$. En caso contrario $a_2 = b_2$ es el único punto en común de R y S, luego $a_1 \neq b_1$ y llamamos T a la única recta paralela a a_1b_1 (y a a_3b_3) que pasa por $a_2 = b_2$.

Si $a_1 - a_2 - a_3$, entonces $a_1 - T - a_3$, pero se cumple que $a_1 \sim_T b_1$ y $a_3 \sim_T b_3$, porque T no puede separar puntos de una recta paralela. Por lo tanto, $b_1 - T - b_3$, luego $b_1 - b_2 - b_3$.

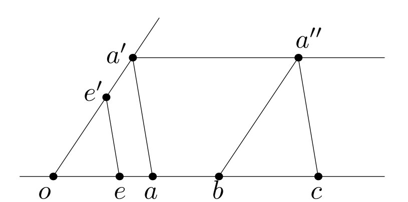
La segunda parte es consecuencia de la primera, pues, para puntos distintos, $a_2 \sim_{a_1} a_3$ equivale a $\neg a_2 - a_1 - a_3$. ■

Ahora necesitamos un resultado técnico sobre la suma geométrica que tiene una traducción algebraica clara:

Teorema 5.40 $\mathrm{Suma}_{oe}^{e'}(abc) \land a \sim_o b \rightarrow o - a - c \land a \neq o \land b \neq o \land a \neq b.$

Esto significa que si sumamos dos números que están al mismo lado del cero (es decir, ambos positivos o ambos negativos), entonces la suma está en ese mismo lado y más lejos del cero que un sumando (y que el otro, por la conmutatividad).

Demostración: Recordemos la construcción de la suma:



Se cumple $a \sim_{a'o} b$ porque no puede ser $a - a'o - b$, ya que la recta $a'o$ corta a ab en o, que por hipótesis no está entre a y b. Por otra parte, $b \sim_{a'o} a''$, porque una recta no separa puntos de otra paralela. Por lo tanto $a \sim_{a'o} a''$, y también $a \sim_{a'a''} o$ (de nuevo por paralelismo). Esto nos permite aplicar el teorema 3.78, que nos da $o - aa' - a''$. Además $c \sim_{aa'} a''$ por paralelismo, luego $o - aa' - c$, que a su vez implica $o - a - c$, así como que los tres puntos son distintos dos a dos. ■

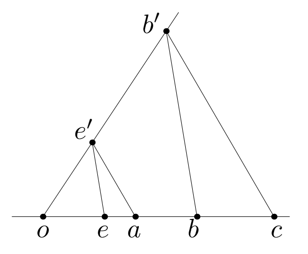
Fijados un origen o y una unidad $e \neq o$, diremos que un punto a de la recta oe es *positivo* si está al mismo lado de o que e, es decir:

$$\mathrm{Pos}_{oe}a \leftrightarrow \mathrm{Ar}_{oe}a \land a \sim_o e.$$

Teorema 5.41 *La suma y el producto de puntos positivos es positiva.*

Demostración: Si $\mathrm{Suma}_{oe}^{e'}(abc) \land \mathrm{Pos}_{oe}a \land \mathrm{Pos}_{oe}b$, entonces $e \sim_o a \land e \sim_o b$, luego $a \sim_o b$, y por el teorema anterior $c \sim_o a \sim_o e$, luego la suma es positiva.

Si $\mathrm{Prod}_{oe}^{e'}(abc) \land \mathrm{Pos}_{oe}a \land \mathrm{Pos}_{oe}b$, recordamos la construcción del producto que muestra la figura. Como $b \sim_o e$, el teorema 5.39 aplicado a la proyección paralela a ee' nos da que $b' \sim_o e'$, y aplicándolo a su vez a la proyección paralela a $e'a$ resulta que $c \sim_o a$, luego $c \sim_o e$ y el producto es positivo. ■



Definimos

$$a <_{oe} b \leftrightarrow \mathrm{Pos}_{oe}(b-a), \qquad a \leq_{oe} b \leftrightarrow a <_{oe} b \lor a = b.$$

Escribiremos $<$ o $\leq$ cuando no sea necesario especificar los puntos o y e.

Teorema 5.42 *Se cumple:*

1. $a \leq a$,
2. $a \leq b \land b \leq a \to a = b$,
3. $a \leq b \land b \leq c \to a \leq c$,
4. $a \leq b \lor b \leq a$,
5. $\mathrm{Ar}_{oe}abc \land b \leq c \to a + b \leq a + c$,
6. $a \geq o \land b \geq o \to ab \geq o$.

DEMOSTRACIÓN: 1) es inmediato. 2) Si fuera $a \neq b$ tendría que cumplirse $\mathrm{Pos}(b-a) \land \mathrm{Pos}(a-b)$, lo cual es imposible, porque, en general, $-x = S_o x$, luego un punto y su opuesto están siempre en lados opuestos respecto de o, y no pueden ser ambos positivos.

3) Si se da alguna igualdad es inmediato y en caso contrario tenemos que $b-a$ y $c-b$ son positivos, luego también lo es su suma, que es $c-a$, luego $a < c$.

4) Si $a = b$ es obvio, y en caso contrario hay que probar que $a-b$ o $b-a$ es positivo, lo cual es obvio, pues ambos son simétricos respecto de o, luego uno de los dos tiene que estar en el mismo lado que e.

5) Si $b = c$ es obvio y si $b \neq c$ basta tener en cuenta que $a+c-(a+b) = c-b$.

6) Si uno de los factores es o es obvio, y en caso contrario basta tener en cuenta que $a > 0$ equivale a que a sea positivo, y ya hemos probado que el producto de puntos positivos es positivo. ■

Ahora es fácil ver que las rectas verifican los axiomas de la teoría CO cuando el relator > 0 se interpreta como Pos_{oe} (o, equivalentemente, como $> o$). Por lo tanto también cumplen todos los teoremas de CO.

El teorema 5.39 implica que toda proyección paralela transforma números positivos en números positivos, y de ahí se deduce inmediatamente que los isomorfismos de cuerpos dados por el teorema 5.36 son de hecho isomorfismos de cuerpos ordenados, luego desde un punto de vista algebraico tenemos una única estructura independiente (salvo isomorfismo) de la elección de o, e.

5.5 Los teoremas de Tales y de Pitágoras

Ya casi estamos en condiciones de demostrar dos de los teoremas más famosos de la geometría euclídea. Sólo nos falta acabar de mostrar cómo la estructura de cuerpo que hemos definido en las rectas nos permite usar los puntos como números y, en particular, como medidas de longitudes de segmentos.

Definición 5.43 Fijados dos puntos $o \neq e$, llamaremos *longitud* de un segmento $\overline{ab}$ al único punto x que cumple $x \sim_o e \wedge \overline{ox} \equiv \overline{ab}$ si es que $a \neq b$, o bien $x = o$ si $a = b$. En principio representaremos por $\ell(\overline{ab})$ la longitud de $\overline{ab}$, pero cuando no haya confusión usaremos la misma notación $\overline{ab}$ para referirnos al segmento o a su longitud.

Teorema 5.44 *Supongamos* Ar_{oe}. *Entonces:*

1. $o \leq \overline{ab}$,

2. $\overline{ab} = o \leftrightarrow a = b$,

3. $\overline{ab} = \overline{cd} \leftrightarrow \overline{ab} \equiv \overline{cd}$.

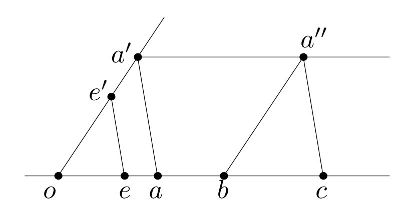
Demostración: Las dos primeras afirmaciones son inmediatas por la definición de longitud. En la tercera hay que entender que en el miembro izquierdo consideramos longitudes y en el derecho segmentos. Para probarla llamamos $x = \ell(\overline{ab})$, $y = \ell(\overline{cd})$, de modo que, por definición $\overline{ox} \equiv \overline{ab}$, $\overline{oy} \equiv \overline{cd}$. (Notemos que esto es cierto incluso si $a = b$ o $c = d$.)

Si $a = b$, ambos miembros de la equivalencia que tenemos que probar son equivalentes a $c = d$, y viceversa, luego podemos suponer que $a \neq b \wedge c \neq d$. Entonces $\overline{ab} \equiv \overline{cd} \leftrightarrow \overline{ox} \equiv \overline{oy} \leftrightarrow x = y$, donde la última equivalencia se debe a la unicidad del transporte de segmentos (teorema 3.35). ■

Ahora necesitamos una observación elemental:

Teorema 5.45 $\mathrm{Suma}_{oe}^{e'}(abc) \to \overline{ob} \equiv \overline{ac}$.

Demostración: Recordamos una vez más la definición de suma:



El teorema 5.6 3) implica que $\overline{ob} \equiv \overline{a'a''} \equiv \overline{ac}$. ■

Teorema 5.46 $\mathrm{Ar}_{oe} \wedge a - b - c \to \overline{ac} = \overline{ab} + \overline{bc}$.

DEMOSTRACIÓN: Hay que entender que el enunciado hace referencia a las longitudes calculadas respecto de o, e. Llamamos $a_1 = \overline{ab}$, $b_1 = \overline{bc}$ y $c_1 = a_1 + b_1$. Tenemos que probar que $c_1 = \overline{ac}$.

Si $a = b$ o $b = c$ la conclusión es trivial, luego suponemos lo contrario. Por definición de longitud, tenemos que $a_1 \sim_o e \sim_o b_1$, luego el teorema 5.40 nos da que $o - a_1 - c_1$. Por definición de longitud $\overline{oa_1} \equiv \overline{ab}$ y por el teorema anterior $\overline{a_1c_1} \equiv \overline{ob_1} \equiv \overline{bc}$. Ahora usamos el teorema 3.3:

$$a - b - c \wedge o - a_1 - c_1 \wedge \overline{ab} \equiv \overline{oa_1} \wedge \overline{bc} \equiv \overline{a_1c_1} \to \overline{ac} \equiv \overline{oc_1},$$

luego $c_1 = \overline{ac}$ por definición de longitud. ■

Observemos ahora que tenemos dos definiciones distintas de $\overline{ab} \leq \overline{cd}$. Por una parte puede entenderse como la relación entre segmentos definida en 3.25, que de momento representaremos por $\overline{ab} \leq_s \overline{cd}$, o la relación de orden entre las longitudes de los segmentos definida en la sección anterior, y que representaremos por $\overline{ab} \leq_l \overline{cd}$. El teorema siguiente demuestra que son equivalentes, por lo que no tendremos necesidad de distinguirlas:

Teorema 5.47 $\mathrm{Ar}_{oe} \to (\overline{ab} \leq_l \overline{cd} \leftrightarrow \overline{ab} \leq_s \overline{cd})$.

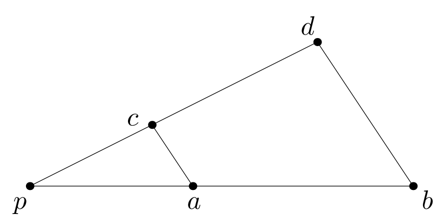
DEMOSTRACIÓN: Si $\overline{ab} \leq_s \overline{cd}$, por definición existe un punto y tal que $c - y - d \wedge \overline{ab} \equiv \overline{cy}$. Entonces, tomando longitudes, $\overline{ab} = \overline{cy} \leq_l \overline{cy} + \overline{yd} = \overline{cd}$, donde hemos usado el teorema anterior.

Por consiguiente, $\overline{ab} <_s \overline{cd} \to \overline{ab} <_l \overline{cd}$, luego, negando la implicación, $\overline{cd} \leq_l \overline{ab} \to \overline{cd} \leq_s \overline{ab}$, que es la implicación que nos faltaba probar, sólo que con otras letras. ■

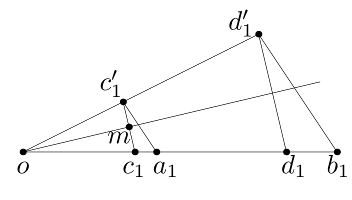
Finalmente:

Teorema 5.48 (Tales)

$$\mathrm{Ar}_{oe} \wedge \mathrm{Col}(pab) \wedge \mathrm{Col}(pcd) \wedge \neg\mathrm{Col}(pac) \wedge \mathrm{Par}(acbd) \to \overline{pa} \cdot \overline{pd} = \overline{pc} \cdot \overline{pb}.$$



DEMOSTRACIÓN: Si $b = p$ entonces $d = p$ por definición de Par, y la conclusión es trivial. Suponemos, pues, que $b \neq p$ y entonces $\neg\mathrm{Col}(pbd)$, porque $b \in pa$, $d \in pc$ y son rectas distintas que se cortan en p.



Llamemos $a_1 = \overline{pa}$, $b_1 = \overline{pb}$, $c_1 = \overline{pc}$, $d_1 = \overline{pd}$. Como $\overline{pq} \equiv \overline{oa_1}$, el teorema 4.7 nos da un punto c_1' tal que $(p, a, c) \equiv (o, a_1, c_1')$. En particular tenemos que $\overline{oc_1} \equiv \overline{pc} \equiv \overline{oc_1'}$, luego si $m = Mc_1c_1'$, se cumple que $om \perp c_1c_1'$, por definición de perpendicularidad y de ángulo recto.

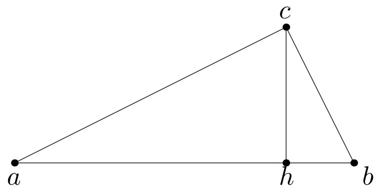
Sea $d_1' = S_{om}d_1$, de modo que $om \perp d_1d_1'$, luego $\mathrm{Par}(c_1c_1'd_1d_1')$, porque dos rectas con una perpendicular común son paralelas. Como S_{om} conserva las congruencias, tenemos que $\overline{od_1'} \equiv \overline{od_1} \equiv \overline{pd}$.

Así pues, los triángulos $\widehat{dpb}$ y $\widehat{d_1'ob_1}$ tienen dos lados y un ángulo iguales, luego por el criterio de congruencia LAL son congruentes. En particular

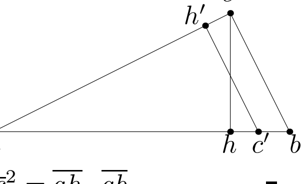
$$\widehat{d_1'b_1o} \equiv \widehat{dpb} \equiv \widehat{cap} \equiv \widehat{c_1'a_1'o},$$

donde la segunda congruencia se cumple por el teorema 5.7 2), que dice que dos paralelas cortan a una misma recta con ángulos iguales. Por la dirección opuesta de ese mismo teorema concluimos que $\mathrm{Par}(a_1c_1'b_1d_1')$. Con esto tenemos que se cumple la definición de $\mathrm{Prod}_{oc_1}^{c_1'}(a_1, d_1, b_1)$ y por 5.37 se cumple $a_1d_1 = c_1b_1$. ■

Teorema 5.49 (Euclides) $\mathrm{Ar}_{oe} \land Racb \land ch \perp ab \land \mathrm{Col}(abh) \rightarrow \overline{ac}^2 = \overline{ah} \cdot \overline{ab}$.



DEMOSTRACIÓN: Tomemos puntos c', h' tales que $c' \sim_a h \land \overline{ac'} \equiv \overline{ac}$ y $h' \sim_a c \land \overline{ah'} \equiv \overline{ah}$. El criterio LAL implica que $(a, h, c) \equiv (a', h', c')$. En particular $Rah'c'$, luego $cb \parallel h'c'$, pues son dos rectas con una perpendicular común. El teorema de Tales nos da que $\overline{ac'} \cdot \overline{ac} = \overline{ah'} \cdot \overline{ab}$, luego $\overline{ac}^2 = \overline{ah} \cdot \overline{ab}$. ■



Teorema 5.50 (Pitágoras) $\mathrm{Ar}_{oe} \land Racb \rightarrow \overline{ab}^2 = \overline{ac}^2 + \overline{bc}^2$.

DEMOSTRACIÓN: Si $\mathrm{Col}(abc)$ las propiedades de los ángulos rectos implican que $a = c \lor b = c$ y la conclusión es trivial. Suponemos, pues, que $\neg\mathrm{Col}(abc)$. Sea h el pie de la perpendicular a ab por c. Por el teorema 4.30 sabemos que $a - h - b$, luego $\overline{ah} + \overline{hb} = \overline{ab}$. Por el teorema anterior $\overline{ac}^2 = \overline{ah} \cdot \overline{ab}$, e intercambiando los papeles de a y b tenemos también $\overline{bc}^2 = \overline{bh} \cdot \overline{ab}$, luego

$$\overline{ac}^2 + \overline{bc}^2 = \overline{ah} \cdot \overline{ab} + \overline{bh} \cdot \overline{ab} = (\overline{ah} + \overline{bh}) \cdot \overline{ab} = \overline{ab}^2.$$ ■

El teorema de Pitágoras impone una condición algebraica a la estructura de cuerpo de las rectas: si a y b son positivos, es fácil construir un triángulo rectángulo con catetos de longitudes a y b, por lo que la longitud c de la hipotenusa cumplirá $a^2 + b^2 = c^2$. Como $a^2 = (-a)^2$, en realidad no hace falta que a y b sean positivos, sino que tenemos:

Teorema 5.51 *Para todo par de puntos $o \neq e$, toda suma de dos cuadrados en la recta oe es un cuadrado.*

En otras palabras, acabamos de probar que las rectas, con las operaciones aritméticas, satisfacen los axiomas de la teoría CP de los cuerpos pitagóricos.

5.6 Coordenadas

Veamos ahora que todo punto de una variedad afín n-dimensional está determinado por n coordenadas. Para construir sistemas de referencia necesitamos algunos resultados previos sobre perpendiculares a variedades afines que no dependen del axioma de las paralelas:

Definición 5.52 Si A es una variedad afín y R es una recta, diremos que son *perpendiculares,* y lo representaremos por $A \perp R$ o $R \perp A$, si se cortan en un punto x y toda recta $S \subset A$ que pase por x cumple $S \perp R$.

Es claro que si A es una recta, esta noción de perpendicularidad coincide con la que ya teníamos definida para rectas.

Es evidente que si $R \perp A$ y $B \subset A$ es una variedad afín que pasa por el punto de corte, entonces $R \perp B$.

Teorema 5.53 *Si A es una variedad afín de dimensión n, $R \subset A$ es una recta y $x \in R$, entonces existe una única variedad $M \subset A$ de dimensión $n-1$ tal que $x \in M$ y $R \perp M$.*

Demostración: Sea $p \in R$ distinto de x y sea $q = S_x p$, de modo que $x = Mpq$. Consideramos la variedad $M = M_A(pq)$ definida en 4.59. Sabemos que es una variedad afín de dimensión $n-1$ y se cumple que $R \perp M$, pues si $S \subset M$ es cualquier recta que pase por x (que es la intersección de M con R) y $a \in S$ es distinto de x, se cumple que $\overline{ap} \equiv \overline{aq}$, por definición de $M_A(pq)$, luego $Raxp$, luego $R \perp S$, luego $R \perp M$.

La unicidad se debe a que si M' cumple lo mismo, todo $u \in M$ distinto de x cumple que $xu \perp pq$, luego $Ruxp$, luego $\overline{up} \equiv \overline{uq}$, luego $u \in M$, luego $M' \subset M$ y, como ambas variedades tienen la misma dimensión, son iguales. ■

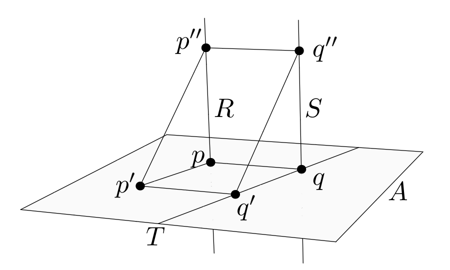
Teorema 5.54 *Si $A = A^n(x_0, \ldots, x_n)$ y R es una recta tal que $x_0 \in R$ y $R \perp x_0x_1 \wedge \cdots \wedge R \perp x_0x_n$, entonces $R \perp A$.*

Esto significa que para que una recta sea perpendicular a una variedad no hace falta comprobar que es perpendicular a todas las rectas que pasan por su punto de intersección, sino que basta que lo sea a las rectas que unen dicho punto con los demás puntos de un generador afínmente independiente de la variedad.

Demostración: Sea $S \subset A$ una recta que pase por x_0, sea $p \in R$ tal que $p \neq x_0$ y sea $q = S_{x_0}p$. Llamamos $B = A^{n+1}(A, p)$. Por hipótesis tenemos que $Rpx_0x_1 \wedge \cdots \wedge Rpx_0x_n$, luego $\overline{x_ip} \equiv \overline{x_iq}$, luego $x_0, \ldots, x_n \in M_B(pq)$, luego $A \subset M_B(pq)$, luego $A \perp pq$. ■

Necesitamos un último resultado sobre perpendicularidad el cual sí que requiere el axioma de las paralelas:

Teorema 5.55 *Si A es una variedad afín y R, S son rectas tales que $R \perp A$, $S \parallel R$ y $S \cap A \neq \varnothing$, entonces $S \perp A$.*



DEMOSTRACIÓN: Sea p el punto de corte entre R y A y sea $q \in S \cap A$. Podemos suponer que $p \neq q$, pues en caso contrario $R = S$. Notemos también que $S \cap A = \{q\}$, pues en caso contrario $S \subset A$ y entonces $R \subset P(S,p) \subset A$, lo cual contradice la perpendicularidad de R.

Tenemos que probar que S es perpendicular a cualquier recta $T \subset A$ que pase por q, pero podemos suponer que $p \notin T$, pues si $p \in T$ sería $T = pq$ y ya sabemos que $S \perp pq$, porque $R \perp pq$ y una perpendicular a una recta lo es a todas sus paralelas (por 5.7 2).

Sea $q' \in T$ un punto distinto de q. Sea p' el punto donde la paralela a T por p corta a la paralela a pq por q'. Sea q'' cualquier punto de S distinto de q y sea p'' el punto en que la paralela a pq por q'' corta a R.

El cuadrilátero $pqq'p'$ es un paralelogramo, luego el teorema 5.6 3) nos da que $\overline{pq} \equiv \overline{p'q'}$ y $\overline{pp'} \equiv \overline{qq'}$. Igualmente $\overline{pq} \equiv \overline{p''q''}$ y $\overline{pp''} \equiv \overline{qq''}$.

Ahora consideramos el cuadrilátero $p'q'q''p''$, que tiene dos lados paralelos $p'q' \parallel p''q''$ y congruentes $\overline{p'q'} \equiv \overline{p''q''}$. Para aplicar 5.6 4) necesitamos garantizar que $p'' - p'q'' - q'$. Esto se sigue del teorema 3.78. En efecto, $p'' \sim_{p'q'} q''$ por paralelismo, y $q' \sim_{p'p''} p'$ porque, el plano $P = pp'p''$, como $q' \sim_{p'p} q$ y $q \sim_{pp''} q''$ por paralelismo, también $q' \sim_P q$ y $q \sim_P q''$, luego $q' \sim_P q''$, luego también $q' \sim_{p'p''} p'$.

La conclusión de 5.6 4) es que $\overline{p'p''} \equiv \overline{q'q''}$, luego $(p, p', p'') \equiv (q, q', q'')$, luego $Rq'qq''$ (porque sabemos que $Rp'pp''$) luego $S \perp T$. ■

Pasamos ya a definir sistemas de referencia. De momento podemos trabajar sin el axioma de las paralelas.

Definición 5.56 Diremos que unos puntos $s, u_1, \ldots, u_n$ son un *sistema de referencia* respecto de unos puntos $0, e$ si cumplen

$$\mathrm{SR}_{oe} s u_1 \cdots u_n \leftrightarrow \mathrm{Ar}_{oe} \wedge \bigwedge_{i=1}^{n} \overline{su_i} \equiv \overline{oe} \wedge \bigwedge_{i \neq j} Ru_i s u_j,$$

es decir, si todos los segmentos $\overline{su_i}$ son unitarios y si las rectas su_i son perpendiculares dos a dos. El punto s es el *origen* del sistema de referencia y las rectas su_i son sus *ejes.*

Notemos que si $m \leq n$ se cumple obviamente que

$$\mathrm{SR}_{oe} s u_1 \cdots u_n \to \mathrm{SR}_{oe} s u_1 \cdots u_m$$

Otra consecuencia es que los puntos de un sistema de referencia son afínmente independientes. En efecto, para $n = 0$ es trivial, y si vale para $n - 1$, el hecho de que $su_n \perp su_i$ para todo $i < n$ implica, por el teorema 5.54, que $su_n \perp A^{n-1}(s, u_1, \ldots, u_{n-1})$, luego en particular $u_n \notin A^{n-1}(s, u_1, \ldots, u_{n-1})$, luego $I^n(s, u_1, \ldots, u_n)$.

Veamos que siempre es posible construir sistemas de referencia:

Teorema 5.57 *Si $o \neq e$, A es una variedad afín n-dimensional y $s \in A$, existen $u_1, \ldots, u_n \in A$ tales que* $\mathrm{SR}_{oe} s u_1 \cdots u_n$ *y* $A = A^n(s, u_1, \ldots, u_n)$.

Demostración: Si $n = 0$ es trivial. Si $n > 0$ tomamos $u_1 \in A$ tal que $\overline{su_1} \equiv \overline{oe}$. Sea $u_1' = S_s u_1$ y sea $A_1 = M_A(u_1 u_1') \subset A$, de modo que A_1 es una variedad afín de dimensión $n-1$ y $su_1 \perp A_1$.

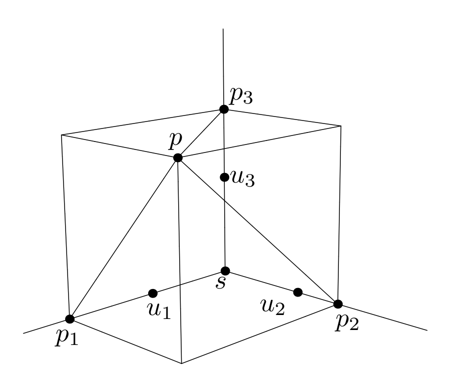
Si $n > 1$ existe un $u_2 \in A_1$ tal que $\overline{su_2} \equiv \overline{oe}$, consideramos $u_2' = S_s u_2$ y $A_2 = M_{A_1}(u_2 u_2')$, que es una variedad afín de dimensión $n-2$ y $su_2 \perp A_2$.

Al cabo de n pasos obtenemos puntos $u_1, \ldots, u_n \in A$ tales que $\overline{su_i} \equiv \overline{oe}$ y cada su_i es ortogonal a las rectas su_j con $j < i$. Por lo tanto $\mathrm{SR}_{oe} s u_1 \cdots u_n$. Como los sistemas de coordenadas son afínmente independientes, necesariamente $A = A^n(s, u_1, \ldots, u_n)$. ■

Definición 5.58 Diremos que un punto p tiene *coordenadas* $x_1, \ldots, x_n$ respecto de o, e y $s, u_1, \ldots, u_n$ si

$$\mathrm{Coord}^{oe}_{su_1\cdots u_n}(p, x_1, \ldots, x_n) \leftrightarrow \mathrm{SR}_{oe} s u_1 \cdots u_n \land p \in A^n(s, u_1, \ldots, u_n) \land$$

$$\bigvee p_1 \cdots p_n \bigwedge_{i=1}^{n} (\mathrm{Col}(s u_i p_i) \land (p_i = p \lor pp_i \perp su_i) \land (o, e, x_i) \equiv (s, u_i, p_i)).$$



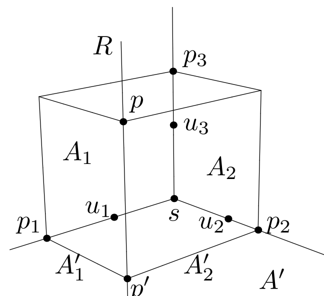
Esto significa que $o \neq e$, que $s, u_1, \ldots u_n$ es un sistema de referencia, que p está en la variedad generada por éste, que cada p_i es el pie de la perpendicular a su_i por p (o el propio p si éste está en el eje) y x_i es el único punto de la recta oe tal que $(o, e, x_i) \equiv (s, u_i, p_i)$ (teoremas 3.17 y 3.20).

En particular $\mathrm{Ar}_{oe} x_1 \cdots x_n$ (es decir, todas las coordenadas están sobre la recta oe).

Es claro que cada punto $p \in A^n(s, u_1, \ldots, u_n)$ tiene unas únicas coordenadas $x_1, \ldots, x_n$ respecto de un sistema de referencia dado, pues p determina las perpendiculares a los ejes, y a su vez sus pies, y a su vez las coordenadas x_i. Lo que no es inmediato es que cada n-tupla de puntos de oe sea la n-tupla de coordenadas de un punto. La prueba requiere el axioma de las paralelas, y previamente demostraremos un resultado auxiliar:

Teorema 5.59 *Tomemos un sistema de referencia* $\mathrm{SR}_{oe} s u_1 \cdots u_n$ *con* $n \geq 1$, *sea* $A = A^n(s, u_1, \ldots, u_n)$ *y para cada* $i = 1, \ldots, n$ *sea* $A_i \subset A$ *una variedad afín de dimensión* $n-1$ *tal que* $su_i \perp A_i$. *Sea* $R = \bigcap_{i=1}^{n-1} A_i$ *(entendiendo que* $R = A$ *si* $n = 1$*. Entonces* R *es una recta,* $R \perp A^{n-1}(s, u_1, \ldots, u_{n-1})$, $R \perp A_n$, $R \parallel su_n$ *y* $\bigcap_{i=1}^{n} A_i$ *es un punto.*

DEMOSTRACIÓN: Lo probamos por inducción sobre n. Si $n = 1$ entonces $A = A^1(s, u_1)$ y $A_1 = \{p\}$, $R = su_1$. Trivialmente $R \perp A^0(s)$, $R \perp A_1$ y $R \parallel su_1$ y A_1 es un punto.



Tomemos $n \geq 2$ y supongamos que el resultado es cierto para $n-1$. Pongamos que $A_i \cap su_i = \{p_i\}$, sea $A' = A^{n-1}(s, u_1, \ldots, u_{n-1})$ y sea $A'_i = A' \cap A_i$, para $i = 1, \ldots, n-1$. Se cumple que $A_i + A' = A$ porque $su_i \subset A'$, pero sólo uno de sus puntos está en A_i, luego $A_i + A' \subset A$ contiene estrictamente a A', luego su dimensión es mayor que $n-1$, luego es n y se da la igualdad.

El teorema 4.57 implica que la dimensión de A'_i es $n-2$, luego podemos aplicar la hipótesis de inducción a A' con $s, u_1, \ldots, u_{n-1}$ y las variedades A'_i. Concluimos que $\bigcap_{i=1}^{n-1} A'_i = \{p'\}$, para un cierto punto p'.

La paralela T_i a su_n por p_i es perpendicular a su_i, porque una perpendicular a una recta lo es a todas sus paralelas, luego está en A_i (porque en la prueba del teorema 5.53 se ve que A_i es de la forma $M_A(s, S_{p_i} s)$ y contiene todas las perpendiculares a su_i). Por lo tanto, la paralela R' a su_n por p cumple $R' \subset A_i$, porque es paralela a T_i, luego $R' \subset P(Y_i, p') \subset A_i$. Por lo tanto tenemos que $R' \subset \bigcap_{i=1}^{n-1} A_i = R$.

Por otra parte $R \cap A' = \bigcap_{i=1}^{n-1} A_i \cap A' = \bigcap_{i=1}^{n-1} A'_i = \{p'\}$. El teorema 4.57 nos da la relación

$$\dim R + \dim A' - \dim(R \cap A') = \dim(R + A'),$$

luego $\dim R + n - 1 - 0 \leq n$, luego $\dim R \leq 1$, luego $R = R'$.

Ahora es inmediato que $R \parallel su_n$ (porque R' lo cumple por construcción). Como su_n es perpendicular a A' (por el teorema 5.54) y a A_n (por hipótesis), el teorema 5.55 nos da que su paralela R cumple lo mismo. Por último, la intersección $\bigcap_{i=1}^{n} A_i = R \cap A_n$ es un punto porque $R \perp A_n$. ■

Ahora ya podemos demostrar que todas las coordenadas determinan puntos:

Teorema 5.60 $\mathrm{Ar}_{oe} x_1 \ldots x_n \land \mathrm{SC}_{oe} s u_1 \cdots u_n \rightarrow$
$\overset{1}{\bigvee} p \in A(s, u_1, \ldots, u_n)\ \mathrm{Coord}^{oe}_{su_1 \cdots u_n} p x_1 \cdots x_n.$

Demostración: La unicidad ya la tenemos probada. Sólo hay que justificar la existencia. Sea $A = A^n(s, u_1, \ldots, u_n)$. Por los teoremas 3.17 y 3.20 existe un único p_i tal que $(o, e, x_i) \equiv (s, u_i, p_i)$. Sea $A_i \subset A$ la variedad de dimensión $n-1$ que cumple $p_i \in A_i \land A_i \perp ou_i$. Por el teorema anterior existe un punto $p \in \bigcap_{i=1}^{n} A_i$. Así $p = p_i$ o bien $pp_i \perp su_i$. Es claro entonces que p tiene por coordenadas a los puntos dados. ■

Así, fijada una recta graduada oe y un sistema de referencia $s, u_1, \ldots, u_n$ en una variedad afín n-dimensional A, cada punto de A se corresponde biunívocamente con una n-tupla de puntos de oe.

En particular, si suponemos los axiomas **A8** y **A9** para un espacio n-dimensional, es decir, los axiomas que establecen que el espacio completo es una variedad afín n-dimensional, entonces lo anterior vale para todo punto del espacio.

Cuando podamos sobrentender la elección de la recta graduada y del sistema de referencia, escribiremos $p = (x_1, \ldots, x_n)$ para indicar que p es el punto de coordenadas $x_1, \ldots, x_n$.

Veamos algunas propiedades técnicas que vamos a necesitar:

Teorema 5.61 *Se cumple:*

1. $\mathrm{Ar}_{oe}xy \land x \leq y \rightarrow \overline{xy} = y - x$,
2. $\mathrm{Ar}_{oe}xy \rightarrow \overline{xy}^2 = (y-x)^2$,
3. *Para* $k \geq 1$,

$$\mathrm{Ar}_{oe}a_1 \cdots a_k \land \bigwedge_{i=1}^{k} (o, e, a_i) \equiv (s, u, p_i) \rightarrow (o, e, a_1, \ldots, a_k) \equiv (s, u, p_1, \ldots, p_k).$$

Demostración: 1) Sea $d = y - x$. Por el teorema 5.45 sabemos que $\overline{od} \equiv \overline{xy}$. Por hipótesis $d \geq o$, luego por definición de longitud $d = \overline{xy}$.

Para probar 2) distinguimos dos casos: $x \leq y$ o $y \leq x$. En el primer caso concluimos por 1), y en el segundo 1) nos da que $\overline{xy} = \overline{yx} = x - y = -(y - x)$, luego también $\overline{xy}^2 = (y-x)^2$.

3) Tenemos que probar que cada segmento formado por dos puntos de entre $o, e, a_1, \ldots, a_k$ es congruente al formado por los puntos correspondientes de $s, u, p_1, \ldots, p_k$, y las únicas congruencias que no se cumplen directamente por hipótesis son las de la forma $\overline{a_i a_j} \equiv \overline{p_i p_j}$, para $i \neq j$, pero basta aplicar el teorema 3.18 a la configuración $\mathrm{Conf5}\begin{pmatrix} o & e & a_i & a_j \\ s & u & p_i & p_j \end{pmatrix}$. ■

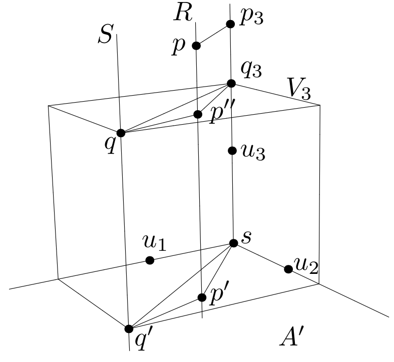
Ahora ya podemos determinar la expresión en coordenadas de la longitud de un segmento arbitrario:

Teorema 5.62 *Fijado un sistema de referencia* $\mathrm{SR}_{oe}su_1\cdots u_n$, *si dos puntos* p *y* q *tienen coordenadas* $p=(x_1,\ldots,x_n)$ *y* $q=(y_1,\ldots,y_n)$, *entonces la longitud del segmento que determinan viene dada por* $\overline{pq}^2=\sum\limits_{i=1}^{n}(y_i-x_i)^2$.

Demostración: Lo probamos por inducción sobre n. Para $n=1$ tenemos que $(o,e,x_1)\equiv(s,u_1,p)$ y $(o,e,y_1)\equiv(s,u_1,q)$. El teorema anterior (tercer apartado) nos da que $\overline{pq}\equiv\overline{x_1y_1}$, luego, por el segundo apartado concluimos que $\overline{pq}^2\equiv\overline{x_1y_1}^2=(y_1-x_1)^2$.

Supongamos cierto el resultado para $n-1$, llamemos $A=A^n(s,u_1,\ldots,u_n)$, sea $A'=A^{n-1}(s,u_1,\ldots,u_{n-1})$, sea $p_i=p$ si $p\in ou_i$ o bien el pie de la perpendicular a ou_i por p. Igualmente, sea $q_i=q$ si $q\in ou_i$ o bien el pie de la perpendicular a ou_i por q. Sea U_i la variedad de dimensión $n-1$ perpendicular a su_i que pasa por p_i y V_i la variedad de dimensión $n-1$ perpendicular a su_i que pasa por q_i. El teorema 5.59 nos da que $R=\bigcap\limits_{i=1}^{n-1}U_i$ y $S=\bigcap\limits_{i=1}^{n-1}V_i$ son rectas paralelas a su_n que cortan a A' en puntos p' y q'.

Observemos que $q\in S\cap V_n$ y, como $V_n\perp su_n$, también $V_n\perp S$. Igualmente, $q'\in A'\cap S$ y, como $A'\perp su_n$, también $A'\perp S$.



Como $p'\in U_i$, para $1\leq i\leq n-1$, tenemos que $p'=p_i$ o bien $p'p_i\perp su_i$, por lo que las coordenadas de p' respecto de $s,u_1,\ldots,u_{n-1}$ son $x_1,\ldots,x_{n-1}$, e igualmente concluimos que las coordenadas de q' son $y_1,\ldots,y_{n-1}$. Por hipótesis de inducción

$$\overline{p'q'}=\sum_{i=1}^{n-1}(y_i-x_i)^2.$$

Si $R\neq su_n$, el pie de la perpendicular a R por q_n es un punto p'' que está en V_n (por estar en una perpendicular a su_n por q_n), luego $V_n\cap R\neq\varnothing$. Más aún, como $su_n\perp V_n$ y $su_n\parallel R$, el teorema 5.55 implica que $R\perp V_n$. Entonces p_np y q_np'' están en el plano que contiene a su_n y a R, luego son coplanares, y ambas son perpendiculares a su_n (porque están en U_n y V_n, respectivamente), luego son paralelas. Por lo tanto p,p_n,q_n,p'' forman un paralelogramo (tal vez degenerado, con $p=p''$, en cuyo caso $p_n=q_n$), luego $\overline{pp''}\equiv\overline{p_nq_n}$. En cualquier caso (tanto si el paralelogramo es degenerado como si no), tenemos que $\overline{pp''}\equiv\overline{p_nq_n}\equiv x_ny_n$, donde la última congruencia se sigue del teorema anterior, pues tenemos que $(o,e,x_n)\equiv(s,u_n,p_n)$ y $(o,e,y_n)\equiv(s,u_n,q_n)$.

Si $R=su_n$ entonces $p=p_n$, tomamos $p''=q_n$ y trivialmente tenemos también que $\overline{pp''}\equiv\overline{p_nq_n}\equiv\overline{x_ny_n}$.

Si $R\neq S$, entonces q,p'',p',q' forman un paralelogramo (tal vez degenerado, con $p''=p'$ y $q=q'$), ya que las rectas $p''q$ y $p'q'$ son coplanares (están en el

plano que contiene a R y a S, que son paralelas), y ambas son perpendiculares a S (por estar contenidas en V_n y A', respectivamente), luego son paralelas. Por lo tanto $\overline{p''q} \equiv \overline{p'q'}$. Si $R = S$ entonces $p'' = q$ y $p' = q'$, y tenemos la congruencia igualmente.

Por último, se cumple $Rpp''q$ (porque $R \perp V_n$), luego por el teorema de Pitágoras concluimos que

$$\overline{pq}^2 = \overline{p''q}^{\,2} + \overline{pp'}^{\,2} = \overline{p'q'}^{\,2} + \overline{x_n y_n}^2 = \sum_{i=1}^{n-1}(y_i - x_i)^2 + \overline{x_n y_n}^2. \qquad \blacksquare$$

Como consecuencia tenemos la caracterización de la congruencia de segmentos en términos de coordenadas:

Teorema 5.63 *Fijado un sistema de referencia, si cuatro puntos tienen coordenadas $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$, $c = (c_1, \ldots, c_n)$, $d = (d_1, \ldots, d_n)$, entonces*

$$\overline{ab} \equiv \overline{cd} \leftrightarrow \sum_{i=1}^{n}(b_i - a_i)^2 = \sum_{i=1}^{n}(d_i - c_i)^2.$$

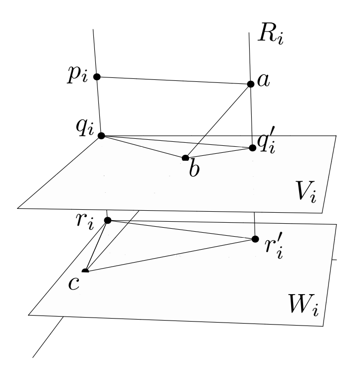
Demostración: Basta tener en cuenta que dos segmentos son congruentes si y sólo si tienen la misma longitud, juntamente con el teorema anterior. $\blacksquare$

Finalmente caracterizamos la relación de ordenación:

Teorema 5.64 *Fijado un sistema de referencia, si tres puntos tienen coordenadas $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$, $c = (c_1, \ldots, c_n)$, entonces*

$$a - b - c \leftrightarrow \bigvee t(\mathrm{Ar}_{oe}t \wedge o \leq t \leq e \wedge \bigwedge_{i=0}^{n} b_i - x_i = t(c_i - a_i)).$$

Demostración: Supongamos que $a - b - c$. El teorema 5.46 nos da que $\overline{ac} = \overline{ab} + \overline{bc}$. Como todas las longitudes son $\geq o$, se cumple que $o \leq \overline{ab} \leq \overline{ac}$. Si $a \neq c$ definimos $t = \frac{\overline{ab}}{\overline{ac}}$, de modo que $o \leq t \leq e$. Así $\overline{ab} = t \cdot \overline{ac}$ y esto vale trivialmente tomando, por ejemplo, $t = e$ si es que $a = c$ (lo que implica $a = b$). Vamos a probar que este t cumple lo requerido.



Sea $A = A^n(s, u_1, \ldots, u_n)$ la variedad afín generada por el sistema de referencia prefijado. Sean p_i, q_i, r_i según la definición de coordenadas para a, b, c, respectivamente, es decir, $p_i = a$ o bien es el pie de la perpendicular a su_i por a, e igualmente con los otros dos puntos. Sean U_i, V_i, W_i las variedades afines de dimensión $n-1$ perpendiculares a su_i por p_i, q_i, r_i, respectivamente. Sea R_i la paralela a su_i que pasa por a. Como ya hemos razonado en otras ocasiones, $R_i \perp V_i$ y $R_i \perp W_i$. Llamamos q'_i y r'_i a los puntos de corte.

Si $\neg\mathrm{Col}(acr'_i)$, podemos aplicar el teorema de Tales al triángulo $\widehat{acr'_i}$. Para ello observamos que $br'_i \parallel cr'_i$ porque ambas rectas son perpendiculares a R_i. El teorema de Tales implica que $\overline{ac} \cdot \overline{aq'_i} = \overline{ar'_i} \cdot \overline{ab} = \overline{ar'_i} \cdot t \cdot \overline{ac}$, luego $\overline{aq'_i} = \overline{ar'_i} \cdot t$ (notemos que $a \neq c$ por la hipótesis de no colinealidad).

Si $\mathrm{Col}(acr'_i)$ hay varias posibilidades, pero todas llevan a la misma conclusión:

Si $a \notin W_i$, tiene que ser $c = r'_i$ (pues c y r'_i están ambos en $W_i \cap R$) y análogamente $b = q'_i$, de donde $\overline{aq'_i} = \overline{ar'_i} \cdot t$.

Si $a \in W_i$ entonces $a = r'_i$ (porque ambos son el punto de corte de R_i con W_i) y, como $a, c \in W_i$, también $b \in W_i$, porque las variedades afines son cerradas para rectas, luego $W_i = V_i$, luego también $a = q'_i$ e igualmente llegamos a que $\overline{aq'_i} = \overline{ar'_i} \cdot t$.

Veamos ahora que $(a, q'_i, r'_i) \equiv (p_i, q_i, r_i)$. En efecto, si $a = p_i$, entonces $R_i = su_i$ y por lo tanto $a = p_i, q'_i = q_i, r'_i = r_i$, con lo que la congruencia se cumple trivialmente. Por lo tanto podemos suponer que $a \neq p_i$, e igualmente que los tres puntos son distintos dos a dos, con lo que definen tres rectas paralelas ap_i, q'_iq_i, r'_ir_i. Son paralelas porque están en el plano de R_i y su_i y son perpendiculares a su_i. Por lo tanto tenemos tres paralelogramos, y sabemos que sus lados opuestos son congruentes, lo que nos da la congruencia de las dos ternas.

Por la definición de coordenadas, $(o, e, a_i) \equiv (s, u_i, p_i)$, $(o, e, b_i) \equiv (s, u_i, q_i)$, $(o, e, c_i) \equiv (s, u_i, r_i)$, y el teorema 5.61 3) nos da que $(p_i, q_i, r_i) \equiv (a_i, b_i, c_i)$. Por lo tanto,

$$\overline{a_ib_i} = \overline{p_iq_i} = \overline{aq'_i} = t \cdot \overline{ar'_i} = t \cdot \overline{p_ir_i} = t \cdot \overline{a_ic_i}.$$

El teorema 5.61 2) nos permite concluir que $b_i - a_i = \pm t(c_i - a_i)$. Sólo falta comprobar que el signo correcto es el positivo. Ahora bien, por el teorema 5.39 vemos que $a - b - c$ implica $a - q'_i - r'_i$, y a su vez $(a, p'_i, r'_i) \equiv (a_i, b_i, c_i)$ implica que $a_i - b_i - c_i$ (teorema 3.13).

Es claro entonces que, o bien $a_i \leq b_i \leq c_i$, o bien $c_i \leq b_i \leq a_i$, luego el signo de $b_i - a_i$ es el mismo que el de $c_i - a_i$, por lo que tiene que ser $b_i - a_i = t(c_i - a_i)$, ya que t es positivo.

Veamos ahora la implicación opuesta. Suponemos que t cumple las condiciones del enunciado. Sea $m = t \cdot \overline{ac}$, de modo que $\overline{oa} = t \cdot \overline{ac}$. Podemos tomar un punto b^* tal que $b^* \sim_a c$ y $\overline{ab^*} \equiv \overline{om}$, es decir, de modo que $\overline{ab^*} = t \cdot \overline{ac}$.

Como $o \leq t \leq e$, se cumple que $\overline{ab^*} \leq \overline{ac}$ (como longitudes, pero también como segmentos), luego $a - b^* - c$. En la prueba de la implicación opuesta hemos visto que el t con que a, b^*, c cumplen el teorema es precisamente el que cumple $\overline{ab^*} = t \cdot \overline{ac}$, es decir, el que tenemos y, por lo tanto, si b_i^* son las coordenadas de b^*, resulta que $b_i^* - a_i = t(c_i - a_i)$, luego $b_i^* = b_i$, luego $b = b^*$, luego $a - b - c$.

■

5.7 Circunferencias

Los axiomas que hemos considerado hasta ahora no permiten demostrar los resultados elementales sobre circunferencias, ni, por consiguiente, los resultados de la geometría elemental que requieren circunferencias para ser demostrados. Terminamos este capítulo presentando un axioma que resuelve este inconveniente.

Definición 5.65 Dados un plano P y dos puntos distintos $c, r \in P$, definimos la *circunferencia* de centro c que pasa por r como el lugar geométrico

$$C_P(c,r) = \{x \mid x \in P \land \overline{cx} \equiv \overline{cr}\}.$$

Los puntos $x \in P$ que cumplen $\overline{cx} < \overline{cr}$ se llaman *puntos interiores* de la circunferencia, mientras que los que cumplen $\overline{cx} > \overline{cr}$ son sus *puntos exteriores.*

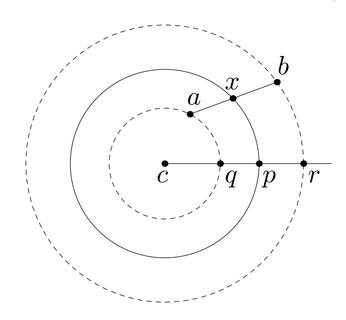
Alternativamente, en lugar de fijar el centro y uno de sus puntos, podemos fijar una recta graduada oe y, para cada $r \in oe$, $r > 0$, definir la circunferencia de centro c y radio r como

$$C_P(c,r) = \{x \mid x \in P \land \overline{cx} = r.$$

El axioma de las circunferencias admite diversos enunciados equivalentes. Escogemos uno que involucra únicamente los conceptos primitivos de la teoría:

Axioma de las circunferencias (AC)

$$c - q - p \land c - p - r \land \overline{ca} \equiv \overline{cq} \land \overline{cb} \equiv \overline{cr} \to \bigvee x(\overline{cc} \equiv \overline{cp} \land a - x - b).$$



Para interpretar este axioma consideramos la circunferencia de centro c que pasa por p contenida en el plano que pasa por c, a, b (o cualquier plano que los contenga si los puntos son colineales). La hipótesis es que $\overline{ca} = \overline{cq} \leq \overline{cp}$, luego a es un punto de la circunferencia o interior a ella. Similarmente $\overline{cb} = \overline{cr} \geq \overline{cp}$, luego b es un punto de la circunferencia o exterior a ella. La conclusión es que hay un punto de la circunferencia entre a y b. Si a o b está en la circunferencia, basta tomar como x el punto que cumpla esto. El caso no trivial se da cuando a es interior y b es exterior. Entonces la existencia de x no puede deducirse de los axiomas que hemos considerado hasta ahora.

En términos de longitudes de segmentos podemos enunciar este axioma (eliminando sus casos triviales) de esta forma:

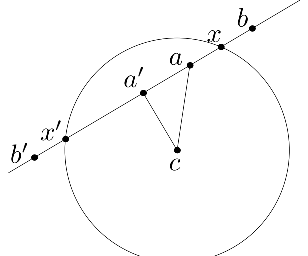
$$\mathrm{Ar}_{oe} r \land \overline{ca} < r < \overline{cb} \to \bigvee x(\overline{cx} = r \land a - x - b).$$

Veamos un enunciado alternativo conceptualmente más simple:

Teorema 5.66 *Las afirmaciones siguientes son equivalentes:*

1. *El axioma de las circunferencias.*
2. *Si una recta pasa por un punto interior de una circunferencia y está contenida en su plano, entonces la corta exactamente en dos puntos.*

Demostración: Supongamos el axioma de las circunferencias y sea R una recta que pase por un punto interior a a una circunferencia de centro c y radio r (y esté contenida en su plano).



Si R pasa por c la conclusión no requiere el axioma de las circunferencias, pues es tanto como decir que en cada una de las semirrectas en que c divide a R hay un único punto x tal que $\overline{cx} \equiv \overline{cr}$, lo cual sabemos que es cierto. Supongamos, pues, que $c \notin R$, sea a' el pie de la perpendicular a R por c, sea $b \in R$ tal que $\overline{ba'} > r$ y sea $b' = S_{a'}b$, de modo que también $\overline{b'a'} = \overline{ba'} > r$.

Observemos que $\overline{bc} > r$, pues dicho segmento es la hipotenusa de un triángulo rectángulo con cateto $\overline{a'b} > r$, e igualmente $\overline{b'c} > r$. Por otra parte, $\overline{a'c} < r$, pues dicho segmento es un cateto de un triángulo rectángulo de hipotenusa $\overline{ac} < r$.

Por el axioma de las circunferencias (en la versión métrica enunciada justo antes de este teorema), existen dos puntos x, x' en la circunferencia tales que $b' - x' - a'$ y $a' - x - b$. Como $x \neq a' \neq x'$, son dos puntos distintos en R y en la circunferencia. No puede haber un tercero, pues si $y \in R$ está en la circunferencia, entonces $\overline{cy} = r$, y el teorema de Pitágoras determina la longitud $\overline{a'y} = \overline{a'x} = \overline{a'x'}$, luego necesariamente $y = x$ o $y = x'$ por la unicidad del transporte de segmentos en semirrectas.

Supongamos ahora la propiedad 2) y veamos que se cumple el axioma de las circunferencias. Tenemos una recta $R = ab$ que pasa por un punto a interior a una circunferencia de centro c y radio r y por otro b que es exterior. Por hipótesis corta a la circunferencia en dos puntos x y x'. Sea a' su punto medio, de modo que $x' - a' - x$. Como están uno a cada lado de a', no perdemos generalidad si suponemos que $x \sim_{a'} b$. Vamos a probar que $a - x - b$.

Para ello observamos que $\overline{a'a} < \overline{a'x} < \overline{a'b}$. En efecto, si $a' = c$, entonces

$$\overline{a'a} = \overline{ca} < r = \overline{cx} = \overline{a'x} < \overline{cb} = \overline{a'b}.$$

Si $a' \neq c$ entonces, como $\overline{cx} = \overline{cx'} = r$, tenemos que $Rca'x$, luego $ca' \perp R$ y tenemos tres triángulos rectángulos $Rca'a$, $Rc'x$, $Rca'b$. Como sus hipotenusas cumplen $\overline{ca} < \overline{cx} < \overline{cb}$ y tienen un cateto en común, el teorema de Pitágoras implica las desigualdades indicadas.

Como $x \sim_{a'} b$, estas desigualdades implican $a' - x - b$, luego si $a = a'$ ya tenemos la relación requerida. Si $a \neq a'$ pero $a \sim_{a'} x \sim_{a'} b$, las desigualdades implican de hecho $a - x - b$, mientras que si $a - a' - b$, entonces $a' - x - b$ implica también $a - x - b$. ■

Terminamos mostrando dos equivalencias más del axioma de las circunferencias, una geométrica y otra algebraica. La segunda afirma que el axioma de las circunferencias es equivalente a que las rectas satisfagan el axioma **E**, es decir, que sean cuerpos euclídeos:

Teorema 5.67 *Las afirmaciones siguientes son equivalentes:*

1. *El axioma de las circunferencias,*
2. *Si* $\mathrm{Ar}_{oe}ab$ *y* $o < b < a$*, existe un triángulo rectángulo con un cateto de longitud* b *e hipotenusa de longitud* a*.*
3. $\mathrm{Ar}_{oe}a \land a \geq o \to \bigvee b(\mathrm{Ar}_{oe}b \land a = b^2)$.

DEMOSTRACIÓN: 1) $\Rightarrow$ 2) Consideremos dos rectas perpendiculares R, S que se corten en un punto x. En S consideremos un punto c tal que $\overline{cx} = b$ y consideremos la circunferencia contenida en el plano determinado por las dos rectas, con centro c y radio a. Como $\overline{cx} = b < a$, el punto x es interior, luego existe $y \in R$ que está en la circunferencia, de modo que $\overline{cy} = a$, y es la hipotenusa del triángulo rectángulo $Rcxy$.

2) $\Rightarrow$ 3) Obviamente 2) implica este hecho:

Si $o < c < a$*, existe un* $b \in oe$ *tal que* $a^2 - b^2 = c^2$*.*

(Simplemente, b es la longitud del otro cateto de un triángulo rectángulo que tenga hipotenusa a y un cateto igual a c. Tomemos ahora $a \geq o$ Si $a = o \lor a = e$, trivialmente $a = a^2$. Si $a > e$ entonces

$$o < \frac{a-e}{2} < \frac{a+e}{2},$$

luego existe un b tal que

$$b^2 = \left(\frac{a+e}{2}\right)^2 - \left(\frac{a-e}{2}\right)^2 = a.$$

Si $o < a < e$ aplicamos la parte ya probada a $1/a > e$, con lo que existe un b tal que $1/a = b^2$, y entonces $a = (1/b)^2$.

3) $\Rightarrow$ 1) Sea R una recta que pase por un punto interior a de una circunferencia de centro c y radio r y que esté contenida en su plano. Si R pasa por c ya hemos razonado en la prueba del teorema anterior que R corta a la circunferencia en dos puntos. En caso contrario sea $a' \in R$ el pie de la perpendicular a R por c. Se cumple que $\overline{ca'} < \overline{ca} < r$, pues $\overline{ca'}$ es el cateto de un triángulo rectángulo de hipotenusa $\overline{ca}$. Por 3) existe un b tal que $b^2 = r^2 - \overline{ca'}^2$. Sean x y x' los dos únicos puntos de R que cumplen $\overline{a'x} = \overline{a'x'} = b$. El teorema de Pitágoras nos da entonces que $\overline{cx} = \overline{cx'} = r$, luego los dos puntos están en R y en la circunferencia. Además son únicos, pues, por el teorema de Pitágoras, cualquier otro debería distar también b de a'. ■

Capítulo VI

La geometría analítica

Estudiamos ahora la relación entre el álgebra y la geometría elemental y demostraremos que ambas teorías son equivalentes en un sentido que tenemos que precisar. No obstante, en primer lugar introducimos el axioma (esquema axiomático, en realidad) que completa la que se conoce como Geometría de Tarski:

6.1 La geometría de Tarski

Para cada número natural $n \geq 2$, la *geometría de Tarski* n-dimensional GT_n es la teoría axiomática sobre el lenguaje formal $\mathcal{L}_S$ cuyos signos eventuales son el relator triádico $a - b - c$ y el relator tetrádico $\overline{ab} \equiv \overline{cd}$ y cuyos axiomas son los siguientes:

A1 $\overline{ab} \equiv \overline{ba}$
A2 $\overline{ab} \equiv \overline{pq} \land \overline{ab} \equiv \overline{rs} \to \overline{pq} \equiv \overline{rs}$
A3 $\overline{ab} \equiv \overline{cc} \to a = b$
A4 $\bigvee x(q - a - x \land \overline{ax} \equiv \overline{bc})$
A5 $a \neq b \land a - b - c \land a' - b' - c'$
$\land \overline{ab} \equiv \overline{a'b'} \land \overline{bc} \equiv \overline{b'c'} \land \overline{ad} \equiv \overline{a'd'} \land \overline{bd} \equiv \overline{b'd'} \to \overline{cd} \equiv \overline{c'd'}$
A6 $a - b - a \to a = b$
A7 $a - p - b \land q - c - b \to \bigvee x(p - x - q \land c - x - a)$
A8$_n$ $\bigvee a_0 \cdots a_n \; I^n(a_0, \ldots, a_n)$
A9$_n$ $\neg \bigvee a_0 \cdots a_{n+1} \; I^{n+1}(a_0, \ldots, a_{n+1})$
A10 $a - d - t \land b - d - c \land a \neq d \to \bigvee xy(a - b - x \land a - c - y \land x - t - y)$
A11 $\bigvee a \bigwedge xy(\alpha(x) \land \beta(y) \to a - x - y) \to \bigvee b \bigwedge xy(\alpha(x) \land \beta(y) \to x - b - y)$.

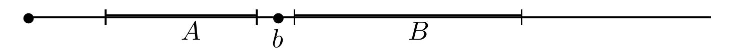
Conviene dar nombre a algunas subteorías: La *geometría de Tarski adimensional* es la teoría axiomática GT que resulta de sustituir el axioma **A8$_n$** por el axioma **A8**, que afirma la existencia de tres puntos no colineales, y eliminar el

axioma $\mathbf{A9}_{\boldsymbol{n}}$, mientras que usaremos la notación GT^{-} y GT_n^{-} para representar la teoría que resulta de eliminar también el axioma **A11**, que es el único que no hemos estudiado hasta ahora.

Se trata en realidad de un esquema axiomático con un caso particular para cada par de fórmulas α y β de $\mathcal{L}_S$. La idea que expresa es que α y β definen dos lugares geométricos:

$$A = \{x \mid \alpha(x)\}, \qquad B = \{y \mid \beta(y)\}.$$

Si alguno de ellos es vacío, el axioma se cumple trivialmente. En caso contrario, la hipótesis afirma que A y B están contenidos en una misma semirrecta de origen a, y de modo que todos los puntos de A están más cerca de a que cualquier punto de B:



La conclusión afirma que existe un punto b situado entre cualquier punto de A y cualquier punto de B. La figura muestra dos lugares geométricos A y B bien separados, pero la relevancia del axioma estriba en que se cumple también aunque A y B "se toquen". Hemos presentado **A11** en esta forma porque es formalmente más simple, pero a partir de él puede probarse la siguiente forma más natural:

Teorema 6.1 *Para toda fórmula $\alpha(x)$ de $\mathcal{L}_S$ (tal vez con más variables libres):*

$$\mathrm{Ar}_{oe}ab \land \alpha(a) \land \neg\alpha(b) \land \bigwedge xy(\mathrm{Ar}_{oe}xy \land \alpha(x) \land \neg\alpha(y) \to x < y)$$

$$\to \bigvee c(\mathrm{Ar}_{oe}c \land \bigwedge xy(\mathrm{Ar}_{oe}xy \land \alpha(x) \land \neg\alpha(y) \to x \leq c \leq y)).$$

Esto significa que si una recta oe puede dividirse en dos lugares geométricos $oe = A \cup B$ no vacíos y de modo que todo punto de A es menor que todo punto de B, entonces existe un punto $c \in oe$ que está situado entre cada punto de A y cada punto de B.

DEMOSTRACIÓN: Aplicamos **A11** a las fórmulas $\alpha'(x)$ y $\beta'(x)$ dadas, respectivamente, por

$$\mathrm{Ar}_{oe}x \land a \leq x \land \alpha(x), \qquad \mathrm{Ar}_{oe}x \land \neg\alpha(x).$$

■

Nota Si añadimos el enunciado del teorema anterior como esquema teoremático a GT^{-} podemos demostrar **A11**.

En efecto, dadas fórmulas $\alpha(x)$ y $\beta(x)$ en las condiciones de **A11**, suponemos que existen puntos e', e tales que $\alpha(e') \land \beta(e)$ (o en caso contrario la conclusión es trivial). Si existe un punto x tal que $\alpha(x) \land \beta(x)$, es fácil ver que $b = x$ cumple lo requerido, así que suponemos lo contrario. Tomamos $o = a$ y aplicamos el teorema anterior a la fórmula $\alpha'(x)$ dada por

$$\bigvee u(\mathrm{Ar}_{oe}xu \land x \leq u \land \alpha(u)).$$

■

Observemos que en GT_n no hemos incluido el axioma de las circunferencias, pero ello se debe a que puede demostrarse a partir de **A11**. En efecto, vamos a probar la forma equivalente dada por el teorema 5.67:

Teorema 6.2 $\mathrm{Ar}_{oe}a \land a \geq o \to \bigvee b(\mathrm{Ar}_{oe}b \land a = b^2)$.

DEMOSTRACIÓN: Podemos suponer que $a > o$, pues para $a = o$ se cumple que $o = o^2$. Aplicamos el axioma **A11** a las fórmulas $\alpha(x)$ y $\beta(x)$ dadas, respectivamente, por

$$\mathrm{Ar}_{oe}x \land x \geq o \land x^2 \leq a, \qquad \mathrm{Ar}_{oe}x \land x \geq o \land a < x^2.$$

El punto a del enunciado de **A11** es en nuestro caso o. Observemos que si se cumple $\alpha(x) \land \beta(y)$, lo que tenemos es que $\mathrm{Ar}_{oe}xy \land x \geq o \land y > o \land x^2 \leq a \leq y^2$. Entonces $0 \leq y^2 - x^2 = (y-x)(y+x)$ con $y+x > 0$. Esto implica[1] que $y - x \geq 0$, es decir, que $o \leq x \leq y$, luego $o - x - y$.

Así pues, se cumple la hipótesis de **A11**, luego concluimos que existe un punto b tal que

$$\bigwedge xy(\mathrm{Ar}_{oe}xy \land x \geq o \land x^2 \leq a < y^2 \to x - b - y).$$

Tomando $x = o$, $y = a + 1$, tenemos que $x^2 \leq a < y^2$, luego $o - b - (a+1)$, con lo que en particular $b \in oe$ y $b \geq o$. Veamos que $b^2 = a$. Supongamos en primer lugar que $b^2 < a$. Entonces $-b^2 + a > o$, luego el teorema 2.13 nos da un $\delta > o$ tal que si $|b - b'| < \delta$ entonces $-b'^2 + a > o$. Tomamos $b' = b + \delta/2$, con lo que $o \leq b < b'$ y $b'^2 < a < (a+1)^2$, luego debería ser $b' - b - (a+1)$ y, como $b' \leq a + 1$, de hecho, $b' \leq b \leq a + 1$, contradicción.

Si, por el contrario, $0 < a < b^2$, como antes existe un $\delta > o$ tal que si $|b - b'| < \delta$ entonces $a < b'^2$. Podemos tomar $b - \delta/2 < b' < b$ de modo que $b' > 0$, con lo que $o^2 \leq a < b'^2$, luego $o - b - b'$, lo que a su vez equivale a $b < b'$, contradicción. ■

Así pues, las rectas de la geometría de Tarski son cuerpos ordenados euclídeos. Más aún, vamos a probar que son cuerpos realmente cerrados:

Teorema 6.3 *Si n es un número natural impar, se cumple:*

$$\mathrm{Ar}_{oe}a_0 \cdots a_{n-1} \to \bigvee x(\mathrm{Ar}_{oe}x \land a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n = o).$$

DEMOSTRACIÓN: Por el teorema 2.15, existe un $M \in oe$ tal que si $x > M$ entonces $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n > 0$, mientras que si $a < -M$ entonces

$$a_0 + a_1a + \cdots + a_{n-1}a^{n-1} + a^n < 0.$$

[1]Aquí estamos usando que las rectas son cuerpos pitagóricos, luego cumplen (las traducciones de) todos los teoremas que hemos demostrado en CP.

Vamos a aplicar el axioma **A11** tomando como $\alpha(x)$ y $\beta(x)$, respectivamente, las fórmulas

$$\mathrm{Ar}_{oe}x \wedge a \leq x \wedge \bigvee z(\mathrm{Ar}_{oe}z \wedge x \leq z \wedge a_0 + a_1 z + \cdots + a_{n-1}z^{n-1} + z^n < 0),$$

$$\mathrm{Ar}_{oe}x \wedge \bigwedge z(\mathrm{Ar}_{oe}z \wedge x \leq z \rightarrow a_0 + a_1 z + \cdots + a_{n-1}z^{n-1} + z^n > 0).$$

Así, si $\alpha(x)\wedge\beta(y)$, existe un z tal que $x \leq z$ y $a_0+a_1z+\cdots+a_{n-1}z^{n-1}+z^n < 0$, luego $\beta(y)$ implica que $z < y$, por lo que $a \leq x < y$, luego $a - x - y$.

En consecuencia, **A11** nos da que existe un b tal que

$$\bigwedge xy(\alpha(x) \wedge \beta(y) \rightarrow x - b - y).$$

Hemos probado que existen puntos x, y que cumplen $\alpha(x) \wedge \beta(y)$, por lo que podemos afirmar que $b \in oe$ y, como también hemos visto que $a \leq x < y$, necesariamente $a \leq x \leq b \leq y$. Vamos a probar que

$$a_0 + a_1 b + \cdots + a_{n-1}b^{n-1} + b^n = o.$$

Veamos que si $z > b$, entonces $a_0+a_1z+\cdots+a_{n-1}z^{n-1}+z^n > 0$. En efecto, en caso contrario $\alpha(z) \wedge \beta(M)$, luego $z \leq b \leq M$, contradicción.

Supongamos ahora que $a_0 + a_1 b + \cdots + a_{n-1}b^{n-1} + b^n > o$. Entonces por el teorema 2.13 existe un $\delta > o$ tal que si $b - \delta < z < b + \delta$ se cumple también $a_0 + a_1 z + \cdots + a_{n-1}z^{n-1} + z^n > 0$. Podemos tomar $b - \delta < z < b$, y entonces $\alpha(a) \wedge \beta(z)$, luego $a \leq b \leq z$, contradicción.

Similarmente, si $a_0+a_1b+\cdots+a_{n-1}b^{n-1}+b^n < o$, el teorema 2.13 aplicado al polinomio cambiado de signo nos permite tomar un punto $b < z$ tal que $a_0+a_1z+\cdots+a_{n-1}z^{n-1}+z^n < o$, pero entonces $\alpha(z)\wedge\beta(M)$, luego $z \leq b \leq M$, contradicción. ■

Así pues, las rectas de GT_n cumplen los axiomas de CRC. Veremos que este hecho nos permitirá probar que, al igual que CRC, la teoría GT_n es consistente, completa y decidible.

6.2 La interpretación de GT_n^- en CP

En esta sección trabajamos en la teoría axiomática CP de los cuerpos ordenados pitagóricos. Aquí vamos a llamar "puntos" a los elementos de R^n, en lugar de "vectores" como hasta ahora.

Definición 6.4 Diremos que un punto $\bar{y} \in R^n$ *está entre* otros dos puntos $\bar{x}, \bar{z} \in R^n$, y lo representaremos por $\bar{x} - \bar{y} - \bar{z}$, si se cumple

$$\bigvee t(0 \leq t \leq 1 \wedge \bar{y} - \bar{x} = t(\bar{z} - \bar{x})),$$

Diremos que el par de puntos $(\bar{x}, \bar{y}) \in R^n \times R^n$ es *congruente* con el par de puntos $(\bar{z}, \bar{w}) \in R^n \times \mathbb{R}^n$, y lo representaremos por $\overline{\bar{x}\bar{y}} \equiv \overline{\bar{z}\bar{w}}$, si se cumple

$$(y_1 - x_1)^2 + \cdots + (y_n - x_n)^2 = (w_1 - z_1)^2 + \cdots + (w_n - z_n)^2.$$

Vamos a demostrar que, para $n \geq 2$, estas dos relaciones cumplen todos los axiomas de GT_n^-. Conviene precisar formalmente esta afirmación, para lo cual damos la definición siguiente:

Definición 6.5 Fijado un número natural $n \geq 2$, A cada fórmula ϕ de $\mathcal{L}_S$ le asignamos una fórmula $\phi^{A,n}$ de $\mathcal{L}_A$ (a la que llamaremos su *traducción analítica*) según el criterio siguiente:

1. A cada variable x de $\mathcal{L}_S$ le asignamos una multivariable $\bar{x} = (x_1, \ldots, x_n)$ de $\mathcal{L}_A$, de modo que si x, y son dos variables distintas, entonces todas las variables $x_1, \ldots, x_n, y_1, \ldots, y_n$ son distintas entre sí.
2. Si ϕ es $x = y$, entonces $\phi^{A,n}$ es $x_1 = y_1 \land \cdots \land x_n = y_n$.
3. Si ϕ es $x - y - z$, entonces $\phi^{A,n}$ es
$$\bigvee t(0 \leq t \leq 1 \land y_1 - x_1 = t(z_1 - x_1) \land \cdots \land y_n - x_n = t(z_n - x_n)).$$
4. Si ϕ es $\overline{xy} \equiv \overline{zw}$, entonces $\phi^{A,n}$ es
$$(y_1 - x_1)^2 + \cdots + (y_n - x_n)^2 = (w_1 - z_1)^2 + \cdots + (w_n - z_n)^2.$$
5. Si ϕ es $\neg\psi$, $\psi \to \chi$, $\bigwedge x\psi$, entonces $\phi^{A,n}$ es, respectivamente,
$$\neg\psi^{A,n}, \quad \psi^{A,n} \to \chi^{A,n}, \qquad \bigwedge x_1 \cdots x_n \, \psi^{A,n}.$$

De 5. se deduce inmediatamente que en CP se demuestra que

$$(\psi \lor \chi)^{A,n} \leftrightarrow \psi^{A,n} \lor \chi^{A,n}, \qquad (\psi \land \chi)^{A,n} \leftrightarrow \psi^{A,n} \land \chi^{A,n},$$
$$(\psi \leftrightarrow \chi)^{A,n} \leftrightarrow (\psi^{A,n} \leftrightarrow \chi^{A,n}), \qquad (\bigvee x \, \psi)^{A,n} \leftrightarrow \bigvee x_1 \cdots x_n \, \psi^{A,n}.$$

En definitiva, las fórmulas $(x - y - z)^{A,n}$ y $(\overline{xy} \equiv \overline{zw})^{A,n}$ son las fórmulas definidas en 6.4 y, en general, $\phi^{A,n}$ es la fórmula de $\mathcal{L}_A$ que afirma de los puntos de R^n (con las definiciones que hemos dado de "estar entre" y de congruencia) lo que ϕ afirma de los puntos del espacio E de GT_n^-.

En estos términos, el resultado que queremos probar se expresa así:

Teorema 6.6 *Si $n \geq 2$, en* CP *se demuestra la traducción (n-dimensional) de todos los axiomas de* GT^-.

Demostración: Conviene observar que todas las demostraciones pueden hacerse en CO excepto la de **A4**, que es el único axioma que requiere de **P** para ser demostrado. La prueba de la mayoría de ellos es trivial. Por ejemplo, consideremos **A3**: $\overline{ab} \equiv \overline{cc} \to a = b$. Su traducción es:

$$\sum_{i=1}^{n} (b_i - a_i)^2 = \sum_{i=1}^{n} (c_i - c_i)^2 \to a_1 = b_1 \land \cdots \land a_n = b_n$$

y, en efecto, esto es demostrable en CO, pues la hipótesis es que $\sum\limits_{i=1}^{n} (b_i - a_i)^2 = 0$, de donde $(b_i - a_i)^2 = 0$, luego $a_i = b_i$.

Los únicos axiomas cuya prueba no es trivial, son **A5**, **A7** y, a lo sumo, **A8**. Analicemos con detalle estos casos. El axioma **A5** es:

$$a \neq b \wedge a{-}b{-}c \wedge a'{-}b'{-}c' \wedge \overline{ab} \equiv \overline{a'b'} \wedge \overline{bc} \equiv \overline{b'c'} \wedge \overline{ad} \equiv \overline{a'd'} \wedge \overline{bd} \equiv \overline{b'd'} \rightarrow \overline{cd} \equiv \overline{c'd'}$$

La traducción de $a \neq b$ es $a_i \neq b_i$ para algún i, luego $\sum_{i=1}^{n}(a_i - b_i)^2 > 0$.

La traducción de $\overline{ab} \equiv \overline{a'b'}$ es $\sum_{i=1}^{n}(a_i - b_i)^2 = \sum_{i=1}^{n}(a'_i - b'_i)^2$, luego el miembro derecho es también no nulo, y por consiguiente $a'_i \neq b'_i$ para algún i.

La traducción de $a - b - c$ es que existe un t tal que $0 \leq t \leq 1$ de modo que $b_i - a_i = t(c_i - a_i)$ para todo i. Como $a_i \neq b_i$ para algún i, tiene que ser, más precisamente, $0 < t \leq 1$.

Similarmente tenemos que existe $0 < t' \leq 1$ tal que $b'_i - a'_i = t'(c'_i - a'_i)$ para todo i.

La traducción de $\overline{bc} \equiv \overline{b'c'}$ es $\sum_{i=1}^{n}(c_i - b_i)^2 = \sum_{i=1}^{n}(c'_i - b'_i)^2$. Desarrollamos el miembro izquierdo:

$$\sum_{i=1}^{n}(c_i - b_i)^2 = \sum_{i=1}^{n}(c_i - a_i - (b_i - a_i))^2 = \sum_{i=1}^{n}\left(\tfrac{1}{t}(b_i - a_i) - (b_i - a_i)\right)^2$$

$$= \left(\tfrac{1}{t} - 1\right)^2 \sum_{i=1}^{n}(b_i - a_i)^2.$$

Haciendo lo mismo con el miembro derecho llegamos a que

$$\left(\tfrac{1}{t} - 1\right)^2 \sum_{i=1}^{n}(b_i - a_i)^2 = \left(\tfrac{1}{t'} - 1\right)^2 \sum_{i=1}^{n}(b'_i - a'_i)^2.$$

Pero sabemos que los sumatorios son iguales y no nulos, luego podemos simplificarlos: $\left(\frac{1}{t} - 1\right)^2 = \left(\frac{1}{t'} - 1\right)^2$. Los términos de dentro de los cuadrados son no negativos, luego podemos eliminar los cuadrados y concluimos que $t = t'$.

También tenemos que

$$\sum_{i=1}^{n}(d_i - b_i)^2 = \sum_{i=1}^{n}(d'_i - b'_i)^2.$$

Desarrollando el miembro izquierdo:

$$\sum_{i=1}^{n}(d_i - b_i)^2 = \sum_{i=1}^{n}(d_i - a_i - (b_i - a_i))^2$$

$$= \sum_{i=1}^{n}(d_i - a_i)^2 + \sum_{i=1}^{n}(b_i - a_i)^2 + 2\sum_{i=1}^{n}(d_i - a_i)(b_i - a_i).$$

Al desarrollar igualmente el segundo miembro podemos cancelar los sumatorios de cuadrados, que sabemos que son iguales, y nos queda:

$$\sum_{i=1}^{n}(d_i - a_i)(b_i - a_i) = \sum_{i=1}^{n}(d_i' - a_i')(b_i' - a_i').$$

Tenemos que demostrar la traducción de $\overline{cd} \equiv \overline{c'd'}$. Ahora bien:

$$\sum_{i=1}^{n}(d_i - c_i)^2 = \sum_{i=1}^{n}(d_i - a_i - (c_i - a_i))^2 = \sum_{i=1}^{n}(d_i - a_i - \tfrac{1}{t}(b_i - a_i))^2$$

$$= \sum_{i=1}^{n}(d_i - a_i)^2 + \tfrac{1}{t^2}\sum_{i=1}^{n}(b_i - a_i)^2 - \tfrac{2}{t}\sum_{i=1}^{n}(d_i - a_i)(b_i - a_i),$$

y hemos demostrado que todas estas expresiones son iguales a las correspondientes con primas, luego $\sum\limits_{i=1}^{n}(d_i - c_i)^2 = \sum\limits_{i=1}^{n}(d_i' - c_i')^2$, como había que probar.

Consideramos ahora **A7**: $a - p - b \wedge q - c - b \to \exists x(p - x - q \wedge c - x - a)$.

La traducción de las hipótesis es que existen $0 \leq t \leq 1$ y $0 \leq t' \leq 1$ tales que $c_i - b_i = t(q_i - b_i)$ y $p_i - b_i = t'(a_i - b_i)$. Debemos encontrar $x_1, \ldots, x_n$ que cumplan $x_i - c_i = u(a_i - c_i)$, $x_i - p_i = u'(q_i - p_i)$, para ciertos $0 \leq u \leq 1$ y $0 \leq u' \leq 1$.

Si $tt' = 1$, necesariamente $t = t' = 1$, en cuyo caso $c_i = q_i$ y $p_i = a_i$ y basta tomar $x_i = p_i$, $u = 1$, $u' = 0$. Supongamos, pues, que $tt' < 1$. Queremos que se cumplan las ecuaciones

$$c_i + u(a_i - c_i) = p_i + u'(q_i - p_i),$$

que equivalen a

$$b_i + t(q_i - b_i) + u(a_i - b_i - t(q_i - b_i)) = b_i + t'(a_i - b_i) + u'(q_i - b_i - t'(a_i - b_i))$$

o también a

$$t(q_i - b_i) + u(a_i - b_i) - ut(q_i - b_i) = t'(a_i - b_i) + u'(q_i - b_i) - u't'(a_i - b_i).$$

Para que se cumpla esto (igualando los coeficientes de $q_i - b_i$ y los de $a_i - b_i$) basta con que $t - ut = u'$, $u = t' - u't'$.

Sustituimos la segunda ecuación en la primera: $t - t'(1 - u')t = u'$, de donde $u' = \frac{t(1-t')}{1-tt'}$. Es claro que eligiendo así u' se cumple $0 \leq u' \leq 1$, y $u = t'(1 - u')$ cumple lo mismo, luego eligiendo $x_i = c_i + u(a_i - c_i) = p_i + u'(q_i - p_i)$ se cumple lo requerido.

El axioma **A8**, es decir, la existencia de tres puntos no colineales, se cumple sin más que definir $a_1 = 1$, $a_i = 0$, para $i \neq 1$, $b_2 = 1$ y $b_i = 0$ para $i \neq 2$, $c_1 = c_2 = 1$, $c_i = 0$ para $i \neq 1, 2$. (Estamos tomando simplemente las n-tuplas de coordenadas $(1, 0, 0 \ldots)$, $(0, 1, 0, \ldots,)$, $(1, 1, 0, \ldots)$.) Comprobar que no cumplen la definición de colinealidad (es decir, que ninguno de los tres puntos está entre los otros dos) no ofrece ninguna dificultad.

Seguidamente demostramos la traducción de **A10**:

$$a - d - t \land c - d - b - \land a \neq d \to \exists xy(a - b - x \land a - c - y \land x - t - y).$$

La traducción de la hipótesis es que existen $0 \leq \lambda \leq 1$, $0 \leq \mu \leq 1$ tales que

$$d_i - c_i = \lambda(b_i - c_i), \quad d_i - a_i = \mu(t_i - a_i).$$

Además, $a \neq d$ se traduce en que tiene que ser $\mu > 0$. Basta tomar

$$x_i = a_i + \frac{1}{\mu}(b_i - a_i), \qquad y_i = a + \frac{1}{\mu}(c_i - a_i).$$

De la propia definición se sigue que $b_i - a_i = \mu(x_i - a_i)$, $c_i - a_i = \mu(y_i - a_i)$, y esto es la traducción de $a - b - x \land a - c - y$. Sólo falta demostrar la traducción de $x - t - y$.

Para ello basta comprobar que $t_i - y_i = \lambda(x_i - y_i)$. En efecto, el miembro izquierdo es

$$t_i - y_i = a_i + \frac{1}{\mu}(d_i - a_i) - a_i - \frac{1}{\mu}(c_i - a_i) = \frac{1}{\mu}(d_i - c_i)$$

Y el miembro derecho:

$$\lambda(x_i - y_i) = \lambda(\frac{1}{\mu}(b_i - a_i) - \frac{1}{\mu}(c_i - a_i)) = \frac{\lambda}{\mu}(b_i - c_i) = \frac{1}{\mu}(d_i - c_i).$$

Finalmente probamos la traducción de **A4** en CP. El axioma es:

$$\exists x(q - a - c \land \overline{ac} \equiv \overline{bc}).$$

Tenemos que definir $x_1, \ldots, x_n$ de modo que exista $0 \leq t \leq 1$ de manera que $a_i - q_i = t(x_i - q_i)$ y además $\sum\limits_{i=1}^{n}(a_i - x_i)^2 = \sum\limits_{i=1}^{n}(b_i - c_i)^2$.

Si $q_i = a_i$ para todo i, entonces la primera parte se cumple trivialmente para cualquier elección de los x_i tomando $t = 0$, y para la segunda tomamos $x_i = a_i - b_i + c_i$.

Supongamos, pues, que algún $q_i \neq a_i$, con lo que tenemos que buscar un $0 < t \leq 1$ y unos x_i de la forma $x_i = q_i + \frac{1}{t}(a_i - q_i)$ y, para que se cumpla la segunda parte:

$$\sum_{i=1}^{n}(b_i - c_i)^2 = \sum_{i=1}^{n}(a_i - x_i)^2 = \sum_{i=1}^{n}(a_i - q_i - \tfrac{1}{t}(a_i - q_i))^2 = \left(1 - \tfrac{1}{t}\right)^2 \sum_{i=1}^{n}(a_i - q_i)^2.$$

El último sumatorio es no nulo porque algún $q_i \neq a_i$, y es un cuadrado porque estamos suponiendo el axioma **P**. Digamos que es A^2, con $A > 0$. El primer sumatorio es también un cuadrado, digamos B^2, con $B \geq 0$. Entonces, si llamamos $C = B/A \geq 0$, todo se reduce a elegir un t que cumpla

$$\left(\frac{1}{t} - 1\right)^2 = C^2, \qquad 0 < t \leq 1.$$

Obviamente sirve $t = 1/(1 + C)$. ■

Con esto hemos definido (para cada número natural n) una interpretación en CP de la geometría de Tarski adimensional (es decir, con los axiomas de dimensión reducidos a la existencia de tres puntos no colineales) en el sentido[2] de [LM 3.28], por lo que podemos afirmar que en CP son demostrables de hecho las traducciones de todos los teoremas de la geometría de Tarski adimensional.

Enseguida probaremos que R^n cumple también los axiomas $\mathbf{A8}_n$ y $\mathbf{A9}_n$, pero para ello necesitamos analizar en qué se traduce en R^n la independencia afín de puntos.

Teorema 6.7 *Si* $n \geq 2$ *y* $m \geq 1$ *son números naturales, en* CP *se demuestra que unos puntos* $\bar{x}_0, \ldots, \bar{x}_m \in R^n$ *son afínmente independientes si y sólo si los vectores* $\bar{x}_1 - \bar{x}_0, \ldots, \bar{x}_m - \bar{x}_0$ *son linealmente independientes, y en tal caso*

$$A^n(\bar{x}_0, \ldots, \bar{x}_m) = \bar{x}_0 + \langle \bar{x}_1 - \bar{x}_0, \ldots, \bar{x}_m - \bar{x}_0 \rangle \,,$$

donde, en general, $\bar{x} + V = \{\bar{y} \mid \bigvee \bar{z} \in V \ \bar{y} = \bar{x} + \bar{z}\}$.

Demostración: Razonamos por inducción sobre m. Para $m = 1$ sabemos que $I^1(\bar{x}_0, \bar{x}_1) \leftrightarrow \bar{x}_0 \neq \bar{x}_1$ (porque esto es la traducción de un teorema de GT^-), y esto equivale a su vez a que $\bar{x}_1 - \bar{x}_0 \neq \bar{0}$, es decir, a que $\bar{x}_1 - \bar{x}_0$ sea linealmente independiente.

Por otra parte, $A^1(\bar{x}_0, \bar{x}_1)$ es la recta que pasa por los dos puntos, formada por todos los puntos $\bar{x}$ que cumplen

$$\bar{x} - \bar{x}_0 - \bar{x}_1 \lor \bar{x}_0 - \bar{x} - \bar{x}_1 \lor \bar{x}_0 - \bar{x}_1 - \bar{x}.$$

En el primer caso existe $0 \leq t \leq 1$ tal que $\bar{x}_0 - \bar{x} = t(\bar{x}_1 - \bar{x})$, luego

$$\bar{x}_0 - \bar{x} = t(\bar{x}_1 - \bar{x}_0) + t(\bar{x}_0 - \bar{x}),$$

luego

$$(t-1)(\bar{x} - \bar{x}_0) = t(\bar{x}_1 - \bar{x}_0).$$

No puede ser $t = 1$, pues entonces sería $\bar{x}_0 = \bar{x}_1$, y estamos suponiendo que no es el caso. Así pues,

$$\bar{x} = \bar{x}_0 + \frac{t}{t-1}(\bar{x}_1 - \bar{x}_0) \in \bar{x}_0 + \langle \bar{x}_1 - \bar{x}_0 \rangle \,.$$

El segundo caso es inmediato y el tercero es análogo al primero.

Recíprocamente, si $\bar{x} \in \bar{x}_0 + \langle \bar{x}_1 - \bar{x}_0 \rangle$, entonces existe un t de manera que $\bar{x} = \bar{x}_0 + t(\bar{x}_1 - \bar{x}_0)$. Si $0 \leq t \leq 1$ ya tenemos que $\bar{x}_0 - \bar{x} - \bar{x}_1$. Si $t > 1$, entonces

$$\bar{x}_1 - \bar{x}_0 = \frac{1}{t}(\bar{x} - \bar{x}_0), \qquad 0 < \frac{1}{t} < 1,$$

luego $\bar{x}_0 - \bar{x}_1 - \bar{x}$.

[2]No exactamente, porque estamos traduciendo cada variable por n variables, mientras que en [LM] se considera que cada variable se traduce en una única variable, pero todos los hechos probados en [LM] sobre interpretaciones se adaptan trivialmente a nuestro contexto.

Por último, si $t < 0$, entonces

$$\bar{x} - \bar{x}_0 = t(\bar{x}_1 - \bar{x}) + t(\bar{x} - \bar{x}_0),$$

luego

$$\bar{x}_0 - \bar{x} = -\frac{t}{1-t}(\bar{x}_1 - \bar{x}), \qquad 0 < -\frac{t}{1-t} < 1,$$

con lo que $\bar{x} - \bar{x}_0 - \bar{x}_1$ y el teorema queda probado para $m = 1$.

Supuesto cierto para m, sabemos que $I^{m+1}(\bar{x}_0, \ldots, \bar{x}_{m+1})$ es equivalente a $I^m(\bar{x}_0, \ldots, \bar{x}_m) \wedge \bar{x}_{m+1} \notin A^m(\bar{x}_0, \ldots, \bar{x}_m)$, es decir, a que $\bar{x}_1 - \bar{x}_0, \ldots, \bar{x}_m - \bar{x}_0$ sean linealmente independientes y que $\bar{x}_{m+1}$ no sea de la forma $\bar{x}_0 + \bar{y}$, con $\bar{y} \in \langle \bar{x}_1 - \bar{x}_0, \ldots, \bar{x}_m - \bar{x}_0 \rangle$, es decir, $\bar{x}_{m+1} - \bar{x}_0 \notin \langle \bar{x}_1 - \bar{x}_0, \ldots, \bar{x}_m - \bar{x}_0 \rangle$, y esto equivale a que $\bar{x}_1 - \bar{x}_0, \ldots, \bar{x}_{m+1} - \bar{x}_0$ sean linealmente independientes.

En tal caso, si llamamos

$$V = \langle \bar{x}_1 - \bar{x}_0, \ldots, \bar{x}_{m+1} - \bar{x}_0 \rangle, \quad A = A^{m+1}(\bar{x}_0, \ldots, \bar{x}_{m+1}),$$

es fácil comprobar que $\bar{x}_0 + V$ es cerrada para rectas. En efecto, si tomamos dos puntos distintos:

$$\bar{u} = \bar{x}_0 + \sum_{i=1}^{m+1} a_i(\bar{x}_i - \bar{x}_0), \qquad \bar{v} = \bar{x}_0 + \sum_{i=1}^{m+1} b_i(\bar{x}_i - \bar{x}_0),$$

por el caso $m = 1$ sabemos que la recta que pasa por ambos está formada por los puntos de la forma $\bar{u} + c(\bar{v} - \bar{u})$, es decir,

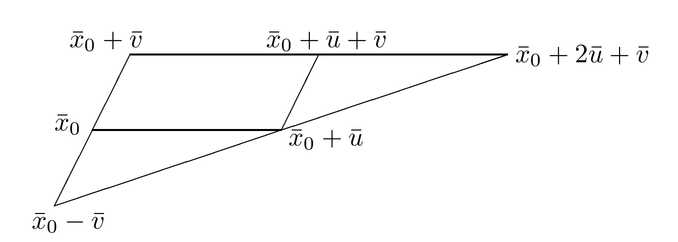
$$\bar{x}_0 + \sum_{i=1}^{m+1} a_i(\bar{x}_i - \bar{x}_0) + c\sum_{i=1}^{m+1} (b_i - a_i)(\bar{x}_i - \bar{x}_0) =$$

$$\bar{x}_0 + \sum_{i=1}^{m+1} (a_i + c(b_i - a_i))(\bar{x}_i - \bar{x}_0) \in \bar{x}_0 + V.$$

Por (la traducción de) el teorema 4.50, concluimos que $\bar{x}_0 + V$ es una variedad afín, que claramente contiene a $\bar{x}_0, \ldots, \bar{x}_{m+1}$. Por consiguiente, tenemos la inclusión $A \subset \bar{x}_0 + V$. Para probar la inclusión contraria hemos de ver que

$$\bar{u} = \bar{x}_0 + \sum_{i=1}^{m+1} a_i(\bar{x}_i - \bar{x}_0) \in A,$$

para lo cual observamos en primer lugar que $\bar{x}_0 + a_i(\bar{x}_i - \bar{x}_0) \in A$, pues es un punto de una recta que pasa por dos puntos de A. Es claro entonces que basta probar que si $\bar{x}_0 + \bar{u}, \bar{x}_0 + \bar{v} \in A$, también $\bar{x}_0 + \bar{u} + \bar{v} \in A$.



En efecto: $\bar{x}_0 - v \in A$ porque está en la recta que pasa por $\bar{x}_0$ y $\bar{x}_0 + \bar{v}$, luego $\bar{x}_0 + 2\bar{u} + \bar{v} \in A$, porque está en la recta que pasa por $\bar{x}_0 + \bar{u}$ y $\bar{x}_0 - v$, luego $\bar{x}_0 + \bar{u} + \bar{v} \in A$, porque está en la recta que pasa por $\bar{x}_0 + \bar{v}$ y $\bar{x}_0 + 2\bar{u} + \bar{v}$. ■

Ahora ya es inmediato:

Teorema 6.8 *En* CP *se demuestra la traducción (n-dimensional) de todos los axiomas de* GT_n^-.

DEMOSTRACIÓN: Sólo falta demostrar $\mathbf{A8}_{\boldsymbol{n}}$ y $\mathbf{A9}_{\boldsymbol{n}}$, pero el primero afirma la existencia de $n+1$ puntos afínmente independientes en R^n, y en efecto, basta considerar $\bar{0}, \bar{e}_1, \ldots, \bar{e}_n$. En cuanto al segundo, afirma que no existen puntos $\bar{x}_0, \ldots, \bar{x}_{n+1}$ afínmente independientes, pero si los hubiera, $\bar{x}_1 - \bar{x}_0, \ldots, \bar{x}_{n+1} - \bar{x}_0$ serían $n+1$ vectores linealmente independientes en R^n, lo cual es imposible. ■

Con esto queda demostrado el teorema siguiente:

Teorema 6.9 *Si* ϕ *es una fórmula de* $\mathcal{L}_S$ *y* $n \geq 2$, *entonces:*

$$si \quad \vdash_{\mathrm{GT}_n^-} \phi \quad también \quad \vdash_{\mathrm{CP}} \phi^{A,n}.$$

Observemos que, si estamos dispuestos a trabajar en la teoría de conjuntos, como es usual, y no en una axiomática *ad hoc* para los cuerpos pitagóricos, todos los argumentos que hemos empleado aquí se traducen trivialmente (y se simplifican) a la demostración de que si R es un cuerpo ordenado pitagórico entonces el producto cartesiano R^n es un modelo de GT_n^-.

Pero el trabajar con una axiomática *ad hoc* nos proporciona un resultado adicional: ahora sabemos que la teoría GT_n^- es consistente, porque si en ella pudiera probarse una contradicción, el teorema anterior nos daría que también puede probarse una contradicción en CP (porque la traducción de una contradicción es una contradicción), pero ya hemos probado que CP es consistente.

Sin embargo, con esto hemos demostrado sólo la parte fácil de la relación entre la versión sintética y la versión analítica de la geometría. Ahora nos disponemos a probar el recíproco del teorema anterior.

Definición 6.10 Consideremos un número natural $n \geq 2$. fijemos dos variables distintas o, e del lenguaje $\mathcal{L}_S$ y establezcamos una correspondencia biunívoca entre las variables restantes de $\mathcal{L}_S$ y las variables de $\mathcal{L}_A$.

A cada término t de $\mathcal{L}_A$ le asignamos como sigue un término t^* de $\mathcal{L}_S$:

1. Si t es una variable de $\mathcal{L}_A$, entonces t^* es la variable de $\mathcal{L}_S$ que le hemos asignado.

2. Si $t = 0, 1$, entonces $t^* = o, e$, respectivamente.

3. Si $t = -t_1$, $t = t_1 + t_2$ o $t = t_1 \cdot t_2$, entonces $t^* = -t_1^*$, $t^* = t_1^* + t_2^*$ o $t^* = t_1^* \cdot t_2^*$, donde ahora $-$, $+$ y $\cdot$ representan el opuesto, la suma y el producto geométricos definidos en GT_n^- respecto de las variables o, e.

A cada fórmula ϕ de $\mathcal{L}_S$ le asociamos como sigue una fórmula ϕ^*:

1. Si ϕ es $t_1 = t_2$ entonces ϕ^* es $t_1^* = t_2^*$.
2. Si ϕ es $t > 0$, entonces ϕ^* es $t^* > o$, donde ahora $>$ es la relación de orden definida en GT_n^- respecto de las variables o y e.
3. Si ϕ es $\neg\psi$ o $\psi \to \chi$, entonces ϕ^* es $\neg\phi^*$ o $\psi^* \to \chi^*$, respectivamente.
4. Si ϕ es $\bigwedge x\psi$, entonces ϕ^* es $\bigwedge x(\mathrm{Ar}_{oe}x \to \psi^*)$.

Es fácil ver entonces que, si las variables libres en ϕ, ψ están entre $x_1, \ldots, x_k$, entonces las variables libres de ϕ^* son las asociadas a las variables libres de ϕ más tal vez o y e. Además en GT_n^- se demuestra:

$$\mathrm{Ar}_{oe}x_1 \cdots x_k \to ((\phi \lor \psi)^* \leftrightarrow \phi^* \lor \psi^*))$$
$$\mathrm{Ar}_{oe}x_1 \cdots x_k \to ((\phi \land \psi)^* \leftrightarrow \phi^* \land \psi^*))$$
$$\mathrm{Ar}_{oe}x_1 \cdots x_k \to ((\phi \leftrightarrow \psi)^* \leftrightarrow (\phi^* \leftrightarrow \psi^*)))$$
$$\mathrm{Ar}_{oe}x_1 \cdots x_k \to ((\bigvee x\psi)^* \leftrightarrow \bigvee x\, (\mathrm{Ar}_{oe}x \land \phi^*))).$$

Ahora es una sencilla rutina comprobar que las traducciones a $\mathcal{L}_S$ de los axiomas de CP son equivalentes a los teoremas de GT_n^- que afirman que cada recta graduada oe es un cuerpo pitagórico con las operaciones que hemos definido geométricamente. Por consiguiente, son teoremas de GT_n^- (aunque en realidad es claro que los axiomas sobre la dimensión no son necesarios). Por consiguiente tenemos definida una interpretación de CP en GT_n^- y según [LM 3.30] se cumple:

Teorema 6.11 *Si ϕ es una fórmula de $\mathcal{L}_A$ con variables libres $x_1, \ldots, x_k$ y $\vdash_{\mathrm{CP}} \phi$, entonces también $\vdash_{\mathrm{GT}_n^-} \mathrm{Ar}_{oe}x_1 \cdots x_k \to \phi^*$.*

Lo que estamos diciendo es que si a partir de los axiomas de CP puede probarse que todos los números $x_1, \ldots x_k$ cumplen lo que dice ϕ, entonces a partir de los axiomas de la geometría sintética podemos demostrar que todos los puntos de una recta graduada oe cumplen ϕ^*, porque podemos probar que los puntos de la recta cumplen (las traducciones de) los axiomas de CP, luego también deben cumplir las consecuencias lógicas de dichos axiomas.

El resultado central es el siguiente:

Teorema 6.12 *Sea $n \geq 2$ un número natural, sea $\phi(x^1, \ldots, x^k)$ una fórmula de $\mathcal{L}_S$ que no contenga a las variables $o, e, s, u_1, \ldots, u_n$, sea $\phi^{A,n}(x_i^j)$ su traducción analítica y sea $\phi^{A,n*}(x_i^j)$ la traducción de ésta de nuevo a $\mathcal{L}_S$. Entonces*

$$\vdash_{\mathrm{GT}_n^-} \mathrm{SR}_{oe}su_1 \cdots u_n \land \bigwedge_{j=1}^{k} \mathrm{Coord}_{su_1\cdots u_n}^{oe} x^j x_1^j \cdots x_n^j \to$$

$$(\phi(x^1, \ldots, x^k) \leftrightarrow \phi^{A,n*}(o, e, x_i^j)).$$

Aquí hay que entender que al traducir de nuevo a $\mathcal{L}_S$ las variables x_i^j se toman distintas de las variables x^j y distintas de $o, e, s, u_1, \ldots, u_n$.

Esto significa que si hemos fijado una recta graduada oe y un sistema de referencia $s, u_1, \ldots, u_n$ y consideramos k puntos $x^1, \ldots, x^k$, entonces dichos puntos cumplen una fórmula ϕ si y sólo si sus coordenadas cumplen $\phi^{A,n*}$.

DEMOSTRACIÓN: Por inducción sobre la longitud de ϕ. Si ϕ es $x = y$, su traducción analítica es $x_1 = y_1 \wedge \cdots \wedge x_n = y_n$, y la traducción geométrica de esta fórmula es ella misma, de modo que lo que hay que probar es que dos puntos son iguales si y sólo si sus coordenadas son iguales, lo cual es ciertamente un teorema de GT_n^-.

Si ϕ es $x - y - z$, entonces su traducción analítica es

$$\exists t(0 \leq t \leq 1 \wedge \bigwedge_{i=1}^{n}(y_i - x_i = t(z_i - x_i))),$$

cuya traducción geométrica es a su vez

$$\exists t(\mathrm{Ar}_{oe}t \wedge o \leq t \leq e \wedge \bigwedge_{i=1}^{n}(y_i - x_i = t(z_i - x_i))).$$

Lo que hay que probar es que se cumple $x - y - z$ si y sólo si las coordenadas de los tres puntos cumplen la relación precedente, pero esto es el teorema 5.64.

Si ϕ es $\overline{xy} \equiv \overline{zw}$ la prueba es análoga, usando esta vez el teorema 5.63.

Si ϕ es $\neg\psi$ basta aplicar la hipótesis de inducción. Como

$$\vdash_{\mathrm{GT}_n^-} \mathrm{SR}_{oe}su_1 \cdots u_n \wedge \bigwedge_{j=1}^{k} \mathrm{Coord}_{su_1\cdots u_n}^{oe} x^j x_1^j \cdots x_n^j \rightarrow$$

$$(\psi(x^1, \ldots, x^k) \leftrightarrow \psi^{A,n*}(o, e, x_i^j)),$$

de aquí se sigue lógicamente

$$\vdash_{\mathrm{GT}_n^-} \mathrm{SR}_{oe}su_1 \cdots u_n \wedge \bigwedge_{j=1}^{k} \mathrm{Coord}_{su_1\cdots u_n}^{oe} x^j x_1^j \cdots x_n^j \rightarrow$$

$$(\neg\psi(x^1, \ldots, x^k) \leftrightarrow \neg\psi^{A,n*}(o, e, x_i^j)).$$

Igualmente se razona si ϕ es de la forma $\psi \rightarrow \chi$. Supongamos finalmente que ϕ es $\bigwedge x\psi(x, x^1, \ldots, x^k)$. La hipótesis de inducción es que, bajo la hipótesis

$$\mathrm{SR}_{oe}su_1 \cdots u_n \wedge \bigwedge_{j=1}^{k} \mathrm{Coord}_{su_1\cdots u_n}^{oe} x^j x_1^j \cdots x_n^j \wedge \mathrm{Coord}_{su_1\cdots u_n}^{oe} x x_1 \cdots x_n$$

se cumple $\psi(x, x^1, \ldots, x^k) \leftrightarrow \psi^{A,n*}(o, e, x_i, x_i^j)$, y lo que tenemos que probar es que bajo las hipótesis

$$\mathrm{SR}_{oe} s u_1 \cdots u_n \wedge \bigwedge_{j=1}^{k} \mathrm{Coord}^{oe}_{su_1 \cdots u_n} x^j x_1^j \cdots x_n^j$$

se cumple

$$\bigwedge x \psi(x, x^1, \ldots, x^k) \leftrightarrow \bigwedge x_1 \cdots x_n (\mathrm{Ar}_{oe} x_1 \cdots x_n \rightarrow \psi^{A,n*}(o, e, x_i, x_i^j)).$$

La prueba es sencilla. Supongamos primero que $\bigwedge x\, \psi(x, x^1, \ldots, x^k)$ y tomemos puntos cualesquiera de la recta graduada $\mathrm{Ar}_{oe} x_1 \cdots x_n$. Sabemos que existe un único punto x cuyas coordenadas son $x_1, \ldots, x_n$ y por hipótesis se cumple $\psi(x, x^1, \ldots, x^k)$, luego la hipótesis de inducción nos da que $\psi^{A,n*}(o, e, x_i, x_i^j)$, que es lo que había que probar.

Recíprocamente, si se cumple $\bigwedge x_1 \cdots x_n (\mathrm{Ar}_{oe} x_1 \cdots x_n \rightarrow \psi^{A,n*}(o, e, x_i, x_i^j))$, tomamos un punto cualquiera x. Aquí usamos los axiomas de dimensión, que establecen que el espacio tiene dimensión n, por lo que x está en $A^n(s, u_1, \ldots, u_n)$, luego tiene unas coordenadas en el sistema de referencia dado, digamos que son $x_1, \ldots, x_n$. Entonces $\mathrm{Ar}_{oe} x_1 \cdots x_n$, luego por hipótesis $\psi^{A,n*}(o, e, x_i, x_i^j)$, y por la hipótesis de inducción, $\psi(x, x^1, \ldots, x^k)$. ■

En particular, sin más que aplicar lo que acabamos de probar al caso de una sentencia (es decir, de una fórmula sin variables libres), tenemos demostrado lo siguiente:

Teorema 6.13 *Si ϕ es una sentencia de $\mathcal{L}_S$ y $n \geq 2$ es un número natural, entonces* $\vdash_{\mathrm{GT}_n^-} \mathrm{Ar}_{oe} \rightarrow (\phi \leftrightarrow \phi^{A,n*}(o, e))$.

Y a su vez:

Teorema 6.14 *Si ϕ es una sentencia de $\mathcal{L}_S$, entonces*

$$\vdash_{\mathrm{GT}_n^-} \phi \qquad \textit{si y sólo si} \qquad \vdash_{\mathrm{CP}} \phi^{A,n}.$$

Demostración: Una implicación es el teorema 6.9. Si suponemos que $\phi^{A,n}$ es demostrable en CP, el teorema anterior nos da que

$$\vdash_{\mathrm{GT}_n^-} \mathrm{Ar}_{oe} \rightarrow (\phi \leftrightarrow \phi^{A,n*}(o, e)).$$

y el teorema 6.11 nos da que $\vdash_{\mathrm{GT}_n^-} \mathrm{Ar}_{oe} \rightarrow \phi^{A,n*}(o, e)$, luego combinando ambos hechos obtenemos que $\vdash_{\mathrm{GT}_n^-} \mathrm{Ar}_{oe} \rightarrow \phi$. Ahora bien, la hipótesis la cumplen dos puntos cualesquiera $o \neq e$, luego $\vdash_{\mathrm{GT}_n^-} \phi$. ■

En resumen, hemos demostrado que una sentencia es demostrable a partir de los axiomas que hemos dado para la geometría sintética n-dimensional si y sólo si su traducción analítica es demostrable a partir de los axiomas de cuerpo pitagórico.

6.3 La interpretación de CP en GT_n^-

Ahora vamos a demostrar un resultado similar, pero que parta de una sentencia de $\mathcal{L}_A$. Necesitamos algunos resultados previos.

Consideremos la fórmula $\mathrm{Suma}_{oe}^{e'}(abc)^{A,n}$, que es una fórmula de $\mathcal{L}_A$ con variables libres o_i, e_i, e'_i, a_i, b_i, c_i, para $i = 1, \ldots, n$. En ella sustituimos

$$o_i = 0, \quad e_i = \begin{cases} 1 & \text{si } i = 1, \\ 0 & \text{si } i \neq 1, \end{cases} \quad e'_i = \begin{cases} 1 & \text{si } i = 2, \\ 0 & \text{si } i \neq 2, \end{cases}$$

así como $a_i = b_i = c_i = 0$ para $i \geq 2$.

El resultado es una fórmula $S(a_1, b_1, c_1)$ con las tres variables indicadas como únicas variables libres. Hacemos lo mismo con $\mathrm{Prod}_{oe}^{e'}(abc)^{A,n}$ y $a >_{oe}^{e'} o$, con lo que obtenemos fórmulas $P(a_1, b_1, c_1)$ y $M(a_1)$.

Teorema 6.15 *Con las definiciones precedentes, se cumple:*

$$\vdash_{\mathrm{CP}} S(a_1, b_1, c_1) \leftrightarrow c_1 = a_1 + b_1, \quad \vdash_{\mathrm{CP}} P(a_1, b_1, c_1) \leftrightarrow c_1 = a_1 \cdot b_1,$$

$$\vdash_{\mathrm{CP}} M(a_1) \leftrightarrow a_1 > 0.$$

DEMOSTRACIÓN: Para calcular explícitamente la fórmula $S(a_1, b_1, c_1)$ tendríamos que escribir explícitamente la fórmula que define la suma geométrica, pero en su lugar podemos razonar de forma más conceptual: Sabemos que $\mathrm{Suma}_{oe}^{e'}(abc)^{A,n}$ es la fórmula de $\mathcal{L}_A$ que afirma que $(c_1, \ldots, c_n)$ son las coordenadas de la suma geométrica de los puntos de coordenadas $(a_1, \ldots, a_n)$ y $(b_1, \ldots, b_n)$ calculada con los puntos de coordenadas $(o_1, \ldots, a_n)$, $(e_1, \ldots, e_n)$ y $(e'_1, \ldots, e'_n)$. Por lo tanto, $S(a_1, b_1, c_1)$ afirma que c_1 es la primera coordenada de la suma de los puntos de coordenadas $(a_1, 0, \ldots, 0)$ y $(b_1, 0, \ldots, 0)$ calculada con los puntos de coordenadas $(0, 0, 0, \ldots, 0)$, $(1, 0, 0, \ldots, 0)$ y $(0, 1, 0, \ldots, 0)$, y queremos probar que $c_1 = a_1 + b_1$.

Observemos que desde el punto de vista de GT_n^- esto es trivial: fijado un sistema de referencia $s, u_1, \ldots, u_n$, los puntos o, e, e' que tienen las coordenadas indicadas son $o = s, e = u_1, e' = u_2$, y las coordenadas de un punto p de la recta oe son $(p, 0, \ldots, 0)$, por lo que es inmediato que las coordenadas de $a + b$ son $(a + b, 0, \ldots, 0)$, pero *no* es esto lo que tenemos que demostrar. Tenemos que trabajar en CP y calcular la suma geométrica de los puntos $(a_1, 0, \ldots, 0)$ y $(b_1, 0, \ldots, 0)$, lo cual es cierta construcción geométrica que, *a priori,* no es inmediato que tenga que dar como resultado $(a_1 + b_1, 0, \ldots, 0)$. Vamos a comprobar que es así.

Por simplicidad no mencionaremos ninguna coordenada de índice mayor que 2, pues todas las que vamos a manejar serán obviamente nulas teniendo en cuenta que todos los puntos de partida las tienen nulas. De acuerdo con la definición de suma geométrica:

1. Consideramos la recta que pasa por los puntos $e = (1, 0)$ y $e' = (0, 1)$, que, partiendo del teorema 6.7, es fácil ver, mediante los razonamientos usuales en geometría analítica, que está formada por los puntos (x, y) tales que $x + y = 1$.

2. Formamos a paralela a esta recta que pasa por $(a_1, 0)$. Es fácil ver que dicha recta está formada por los puntos (x, y) tales que $x + y = a_1$ (por ejemplo, usando 6.7 para probar que éstos son los puntos de la recta que pasa por $(a_1, 0)$ y $(a_1 - 1, 1)$, y luego comprobando que el sistema formado por las dos ecuaciones no tiene solución).

3. Buscamos el corte de esta recta con la que pasa por $(0, 0)$ y $(0, 1)$, que está formada por los puntos que cumplen $x = 0$, con lo que el punto de corte es $(0, a_1)$.

4. Consideramos la recta que pasa por $(0, 0)$ y $(1, 0)$, que tiene ecuación $y = 0$, y formamos su paralela por $(0, a_1)$, que tiene ecuación $y = a_1$.

5. Calculamos la paralela a la recta $x = 0$ que pasa por $(b_1, 0)$, que tiene por ecuación $x = b_1$.

6. Calculamos la intersección de las dos últimas rectas, que es (b_1, a_1).

7. Calculamos la paralela a la recta $x + y = 1$ que pasa por (b_1, a_1), que es fácil ver que es $(x + y = a_1 + b_1)$.

8. La suma es la intersección de esta recta con $y = 0$, es decir, el punto $(a_1 + b_1, 0)$.

Esto prueba que $S(a_1, b_1, c_1) \leftrightarrow c_1 = a_1 + b_1$.

El mismo procedimiento se aplica al caso de P. Lo esbozamos dejando los detalles a cargo del lector: primero se calculan las rectas $x+y = 1$ y $x+y = a_1$, luego la paralela a la primera por $(b_1, 0)$, que es $a + y = b_1$ y que corta a $x = 0$ en $(0, b_1)$, luego la paralela a la segunda por este punto, que es $x + a_1 y = a_1 b_1$, y el producto es el punto de corte de esta recta con $y = 0$, es decir, $(a_1 b_1, 0)$.

Para M usamos que $a > o \leftrightarrow \neg a - o - e$. Al traducir y sustituir las coordenadas de o, e, e' y las coordenadas nulas de índices mayores que 1 obtenemos que

$$M(a_1) \leftrightarrow \neg \bigvee t(0 \leq t \leq 1 \land -a_1 = t(1 - a_1)).$$

Ahora bien, es fácil ver que la condición $-a_1 = t(1 - a_1)$ (que es equivalente a $(t - 1)a_1 = t$), con $0 \leq t \leq 1$, equivale a que $a_1 \leq 0$, luego $M(a_1) \leftrightarrow a_1 > 0$. ■

Nota Lo que hemos probado es que en CP se demuestra que si

$$A = A^1(\bar{0}, \bar{e}_1) = \{\bar{x} \mid x_2 = \cdots = x_n = 0\},$$

la aplicación $F : \mathbb{R} \longrightarrow A$ dada por $F(a) = (a, 0, \ldots, 0)$ es un isomorfismo de cuerpos ordenados. ■

Consideremos ahora una fórmula arbitraria $\phi(x^1, \ldots, x^k)$ de $\mathcal{L}_A$. Podemos calcular su traducción $\phi^*(o, e, x^1, \ldots, x^k)$ a $\mathcal{L}_S$ y luego volver a $\mathcal{L}_A$ mediante

$\phi^{*A,n}(o_i, e_i, x_i^1, \ldots, x_i^k)$, donde $i = 1, \ldots, n$. Llamaremos $\phi^{*n}(x^1, \ldots, x^n)$ a la fórmula que resulta de sustituir en $\phi^{*A,n}$ las variables libres con el criterio siguiente:

1. $o_i = 0$,
2. $e_1 = 1$ y $e_i = 0$ para $i > 1$,
3. $x_1^j = x^j$ y $x_i^j = 0$ para $i > 1$.

Teorema 6.16 *Si* $n \geq 2$ *y* $\phi(x^1, \ldots, x^k)$ *es cualquier fórmula de* $\mathcal{L}_A$ *cuyas variables libres estén entre las indicadas, entonces* $\vdash_{\mathrm{CP}} \phi \leftrightarrow \phi^{*n}$.

DEMOSTRACIÓN: Vamos a probar el teorema bajo la hipótesis adicional de que toda subfórmula atómica de ϕ es de la forma $z = 0$, $z = 1$, $z = x$, $z = x+y$, $z = xy$ o $x > 0$, donde x, y, z son variables cualesquiera. Luego veremos que toda fórmula ϕ es lógicamente equivalente a otra en estas condiciones. Razonamos por inducción sobre la longitud de ϕ.

Si ϕ es de la forma $x^1 = 0$, entonces ϕ^* es $x^1 = o$, por lo que $\phi^{*A,n}$ es $x_1^1 = o_1 \wedge \cdots \wedge x_n^1 = o_n$ y ϕ^{*n} es $x^1 = 0 \wedge 0 = 0 \wedge \cdots \wedge 0 = 0$, que es equivalente a $x^1 = 0$.

Los casos $x^1 = e$ y $x^1 = x^2$ son similares, y los casos $x^3 = x^1 + x^2$, $x^3 = x^1 x^2$, $x_1 > 0$ se cumplen por el teorema anterior.[3]

Los casos en que ϕ es de la forma $\neg\psi$ o $\psi \rightarrow \chi$ no ofrecen ninguna dificultad. Supongamos por último que ϕ es de la forma $\bigwedge x\, \psi(x, x^1, \ldots, x^k)$. Entonces ϕ^* es $\bigwedge x(\mathrm{Col}(oex) \rightarrow \psi^*(x, x^1, \ldots, x^k))$, luego, usando 6.7, resulta que $\phi^{*A,n}$ es

$$\bigwedge x_1 \cdots x_n (\bigvee t \bigwedge_{i=1}^{n} x_i - o_i = t(e_i - o_i) \rightarrow \psi^{*A,n}(x_i, x_i^1, \ldots, x_i^k)).$$

Al hacer las sustituciones según la definición de ϕ^{*n} obtenemos

$$\bigwedge x_1 \cdots x_n (\bigvee t(x_1 = t \wedge \bigwedge_{i=2}^{n} x_i = 0) \rightarrow \psi^{*A,n}(x_i, x^1, \ldots, x^k)),$$

que claramente equivale a $\bigwedge x\, \psi^{*n}(x, x^1, \ldots, x^k)$. Por hipótesis de inducción, esta fórmula es a su vez equivalente a $\bigwedge x\, \psi(x, x^1, \ldots, x^k)$. ■

Finalmente podemos probar:

[3] En los términos del teorema anterior, para el caso $x^3 = x^1 + x^2$, tendríamos que ϕ^* sería $\bigvee e'(\neg\mathrm{Col}(oee') \wedge \mathrm{Suma}_{oe}^{e'}(x^1, x^2, x^3))$ y a su vez $\phi^{*A,n}$ sería

$$\bigvee e_1' \cdots e_n'(\neg\mathrm{Col}(oee')^{A,n} \wedge \mathrm{Suma}_{oe}^{e'}(x^1, x^2, x^3)^{A,n}).$$

Ahora bien, el teorema de GT_n^- que afirma que la suma no depende de la elección de e' se traduce en el teorema de CP que afirma que la fórmula anterior no depende de la elección de los e_i' (siempre que cumplan la hipótesis de no colinealidad), y es claro que cuando sustituimos las o_i y las e_i según la definición de $\phi^{*A,n}$, una elección válida para las e_i' es tomar $e_2' = 1$ y las restantes nulas, por lo que $\phi^{*A,n} \leftrightarrow S(x^1, x^2, x^3) \leftrightarrow x^3 = x^1 + x^2$. Lo mismo se aplica a los otros dos casos.

Teorema 6.17 *Sea ϕ una sentencia de $\mathcal{L}_A$ y $n \geq 2$. Entonces,*

$$\vdash_{\mathrm{GT}_n^-} \bigwedge oeo'e'(o \neq e \land o' \neq e' \to (\phi^*(o,e) \leftrightarrow \phi^*(o',e'))),$$

$$\vdash_{\mathrm{CP}} \phi \leftrightarrow (\bigwedge oe(o \neq e \to \phi^*(o_i,e_i)))^{A,n} \leftrightarrow (\bigvee oe(o \neq e \land \phi^*(o_i,e_i)))^{A,n},$$

y las afirmaciones siguientes son equivalentes:

1. $\vdash_{\mathrm{GT}_n^-} \bigwedge oe(o \neq e \to \phi^*(o,e))$,
2. $\vdash_{\mathrm{GT}_n^-} \bigvee oe(o \neq e \to \phi^*(o,e))$,
3. $\vdash_{\mathrm{CP}} \phi$.

Demostración: Veamos en primer lugar que toda fórmula $\phi(x^1,\ldots,x^k)$ es lógicamente equivalente a otra $\bar{\phi}$ con las mismas variables libres cuyas subfórmulas atómicas son todas de la forma $z=0$, $z=1$, $z=x$, $z=x+y$, $z=xy$ o $x>0$, donde x,y,z son variables cualesquiera, así como que $\vdash_{\mathrm{GT}_n^-} (\phi^* \leftrightarrow \bar{\phi}^*)$.

Para ello probamos en primer lugar que para todo término $t(x^1,\ldots,x^k)$ de $\mathcal{L}_A$ existe una fórmula $\phi_t(x,x^1,\ldots,x_k)$ con subfórmulas atómicas de los tipos indicados tal que

$$\vdash_{\mathrm{CP}} (x=t \leftrightarrow \phi_t), \qquad \vdash_{\mathrm{GT}_n^-} (x=t^* \leftrightarrow \phi_t^*).$$

En efecto, razonando por inducción sobre la longitud de t, si t es una variable x^1, o bien 0, o bien 1, basta tomar como $\phi_t(x,t)$ la fórmula $x=t$, con lo que t^* es x^1, o, e, respectivamente y ϕ_t^* es $x=t^*$.

Si t es t_1+t_2, tomamos como ϕ_t la fórmula $\bigvee yz(x=y+z \land \phi_{t_1}(y) \land \phi_{t_2}(z))$ y es claro que cumple lo requerido. Si t es $t_1 \cdot t_2$ se razona análogamente. Por último, si t es $-t_1$ tomamos como ϕ_t la fórmula $\bigvee yz(y=0 \land y=x+z \land \phi_{t_1}(z))$.

Pasamos ya a la construcción de la fórmula $\bar{\phi}$, también por inducción sobre la longitud de ϕ. Para fórmulas atómicas de tipo $t>0$ definimos $\bar{\phi}$ como

$$\bigvee x(x>0 \land \phi_t(x,x^1,\ldots,x^k)),$$

que claramente cumple lo requerido. Análogamente se trata el caso de $t_1=t_2$. Si ϕ es $\neg\psi$, $\psi \to \chi$ o $\bigwedge x\,\psi$, definimos $\bar{\phi}$ como $\neg\bar{\psi}$, $\bar{\psi} \to \bar{\chi}$ y $\bigwedge x\,\bar{\psi}$, respectivamente, y también es fácil comprobar que cumplen lo requerido.

Recordemos ahora el teorema 5.36, que afirma que dos rectas cualesquiera son isomorfas como cuerpos ordenados. Más precisamente, esto significa que existe una fórmula $\Phi_{oe}^{o'e'}(x,y)$ que define un isomorfismo de cuerpos ordenados entre las rectas oe y $o'e'$, es decir, tal que

$$\vdash_{\mathrm{GT}_n^-} \bigwedge oeo'e'(o \neq e \land o' \neq e' \to \cdots),$$

donde los puntos suspensivos representan la conjunción de las fórmulas siguientes:

1. $\bigwedge x(\mathrm{Ar}_{oe}x \to \overset{1}{\bigvee} y(\mathrm{Ar}_{o'e'}y \land \Phi_{oe}^{o'e'}(x,y)))$,

2. $\bigwedge y(\mathrm{Ar}_{oe} y \rightarrow \overset{1}{\bigvee} x(\mathrm{Ar}_{o'e'} x \wedge \Phi_{oe}^{o'e'}(x, y)))$,
3. $\bigwedge x_1 x_2 x_3 y_1 y_2 y_3(\mathrm{Ar}_{oe} x_1 x_2 x_3 \wedge \mathrm{Ar}_{o'e'} y_1 y_2 y_3 \wedge \Phi_{oe}^{o'e'}(x_1, y_1)$
$\wedge\, \Phi_{oe}^{o'e'}(x_2, y_2) \wedge \Phi_{oe}^{o'e'}(x_3, y_3) \rightarrow (x_3 = x_1 + x_2 \leftrightarrow y_3 = y_1 + y_2))$,
4. $\bigwedge x_1 x_2 x_3 y_1 y_2 y_3(\mathrm{Ar}_{oe} x_1 x_2 x_3 \wedge \mathrm{Ar}_{o'e'} y_1 y_2 y_3 \wedge \Phi_{oe}^{o'e'}(x_1, y_1)$
$\wedge\, \Phi_{oe}^{o'e'}(x_2, y_2) \wedge \Phi_{oe}^{o'e'}(x_3, y_3) \rightarrow (x_3 = x_1 \cdot x_2 \leftrightarrow y_3 = y_1 \cdot y_2))$,
5. $\bigwedge x_1 x_2 y_1 y_2(\mathrm{Ar}_{oe} x_1 x_2 \wedge \mathrm{Ar}_{o'e'} y_1 y_2 \wedge \Phi_{oe}^{o'e'}(x_1, y_1) \wedge \Phi_{oe}^{o'e'}(x_2, y_2) \rightarrow$
$(x_1 \leq x_2 \leftrightarrow y_1 \leq y_2)$.
6. $\Phi_{oe}^{o'e'}(o, o') \wedge \Phi_{oe}^{o'e'}(e, e')$.

Observemos ahora que si $\bar{\phi}(x^1, \ldots, x^k)$ es cualquier fórmula de $\mathcal{L}_A$ cuyas subfórmulas atómicas sean de los tipos $z = 0$, $z = 1$, $z = x$, $z = x + y$, $z = xy$ o $x \leq y$, entonces

$$\vdash_{\mathrm{GT}_n^-} \bigwedge oeo'e'(o \neq e \wedge o' \neq e' \rightarrow \bigwedge x^1 \cdots x^n y^1 \cdots y^n(\mathrm{Ar}_{oe} x^1 \cdots x^k \wedge \mathrm{Ar}_{o'e'} y^1 \cdots y^k$$

$$\wedge \bigwedge_{i=1}^{k} \Phi_{oe}^{o'e'}(x^i, y^i) \rightarrow (\bar{\phi}^*(o, e, x^1, \ldots, x^k) \leftrightarrow \bar{\phi}^*(o', e', y^1, \ldots, y^k)))).$$

En efecto, basta razonar por inducción sobre la longitud de $\bar{\phi}$. El hecho de que Φ sea un isomorfismo implica inmediatamente el resultado para las fórmulas atómicas, y el resto de la inducción no presenta ninguna dificultad. En el caso en que $\bar{\phi}$ es $\bigwedge x \bar{\psi}$ hay que usar la biyectividad de Φ expresada en las condiciones 1. y 2.

Con esto estamos ya en condiciones de demostrar el teorema. Partimos de una sentencia ϕ de $\mathcal{L}_A$, a partir de la cual podemos construir la sentencia $\bar{\phi}$ tal que $\vdash_{\mathrm{CP}} (\phi \leftrightarrow \bar{\phi})$ y $\vdash_{\mathrm{GT}_n^-} (\phi^* \leftrightarrow \bar{\phi}^*)$. Según acabamos de probar, tenemos además que

$$\vdash_{\mathrm{GT}_n^-} \bigwedge oeo'e'(o \neq e \wedge o' \neq e' \rightarrow (\bar{\phi}^*(o, e) \leftrightarrow \bar{\phi}^*(o', e'))),$$

luego también

$$\vdash_{\mathrm{GT}_n^-} \bigwedge oeo'e'(o \neq e \wedge o' \neq e' \rightarrow (\phi^*(o, e) \leftrightarrow \phi^*(o', e'))),$$

como había que probar. Esto implica ya la equivalencia entre las afirmaciones 1. y 2. del enunciado, así como que

$$\vdash_{\mathrm{GT}_n^-} \bigwedge oe(o \neq e \rightarrow \phi^*(o, e)) \leftrightarrow \bigvee oe(o \neq e \wedge \phi^*(o, e)),$$

y el teorema 6.9 implica entonces que

$$\vdash_{\mathrm{CP}} (\bigwedge oe(o \neq e \rightarrow \phi^*(o_i, e_i)))^{A,n} \leftrightarrow (\bigvee oe(o \neq e \wedge \phi^*(o_i, e_i)))^{A,n},$$

como había que probar. Como también tenemos

$$\vdash_{\mathrm{GT}_n^-} \bigwedge oeo'e'(o \neq e \wedge o' \neq e' \rightarrow (\phi^*(o, e) \leftrightarrow \bar{\phi}^*(o', e'))),$$

aplicando de nuevo 6.9 tenemos que

$$\vdash_{\mathrm{CP}} \bigwedge o_1 \cdots o_n e_1 \cdots e_n o'_1 \cdots o'_n e'_1 \cdots e'_n (\bigvee_{i=1}^n o_i \neq e_i \land \bigvee_{i=1}^n o'_i \neq e'_i \rightarrow$$

$$(\phi^{*A,n}(o_i, e_i) \leftrightarrow \bar{\phi}^{*A,n}(o'_i, e'_i))).$$

Ahora sustituimos $o'_i = e'_i = 0$ para todo i, salvo $e'_1 = 1$, con lo que obtenemos

$$\vdash_{\mathrm{CP}} \bigwedge o_1 \cdots o_n e_1 \cdots e_n (\bigvee_{i=1}^n o_i \neq e_i \rightarrow (\phi^{*A,n}(o_i, e_i) \leftrightarrow \bar{\phi}^{*n})).$$

Por el teorema 6.16 esto equivale a

$$\vdash_{\mathrm{CP}} \bigwedge o_1 \cdots o_n e_1 \cdots e_n (\bigvee_{i=1}^n o_i \neq e_i \rightarrow (\phi^{*A,n}(o_i, e_i) \leftrightarrow \bar{\phi}))$$

y, por construcción de $\bar{\phi}$, a su vez, tenemos que

$$\vdash_{\mathrm{CP}} \bigwedge o_1 \cdots o_n e_1 \cdots e_n (\bigvee_{i=1}^n o_i \neq e_i \rightarrow (\phi^{*A,n}(o_i, e_i) \leftrightarrow \phi)),$$

o también:

$$\vdash_{\mathrm{CP}} (\bigwedge oe(o \neq e \rightarrow \phi^*(o_i, e_i)))^{A,n} \leftrightarrow \phi,$$

que es lo que faltaba probar de la primera parte del teorema. Por lo tanto, $\vdash_{\mathrm{CP}} \phi$ es equivalente a

$$\vdash_{\mathrm{CP}} (\bigwedge oe(o \neq e \rightarrow \phi^*(o_i, e_i)))^{A,n},$$

que por el teorema 6.14 es equivalente a su vez a

$$\vdash_{\mathrm{GT}_n^-} \bigwedge oe(o \neq e \rightarrow \phi^*(o, e)).$$

■

Lo que expresa el teorema anterior es que las fórmulas $\phi^*(o, e)$ expresan que las rectas poseen la propiedad algebraica dada por ϕ, y que ϕ se puede demostrar en CP si y sólo si en GT_n^- se puede probar que las rectas, como cuerpos ordenados, cumplen la propiedad ϕ.

Por ejemplo, el teorema 5.67 afirma que el axioma de las circunferencias **AC** y el axioma euclídeo **E** definido en 2.8 cumplen la relación

$$\vdash_{\mathrm{GT}_n^-} \mathbf{AC} \leftrightarrow \bigwedge oe(o \neq e \rightarrow \mathbf{E}^*(o, e)).$$

Por lo tanto, el teorema anterior nos da que

$$\vdash_{\mathrm{CP}} \mathbf{AC}^{A,n} \leftrightarrow \mathbf{E}.$$

Esto nos da inmediatamente las extensiones siguientes de 6.14 y del teorema anterior:

Teorema 6.18 *Si ϕ es una sentencia de $\mathcal{L}_S$, entonces*

$$\vdash_{\mathrm{GT}_n^-+\mathbf{AC}} \phi \quad \textit{si y sólo si} \quad \vdash_{\mathrm{CE}} \phi^{A,n}.$$

Si ϕ es una sentencia de $\mathcal{L}_A$, entonces

$$\vdash_{\mathrm{CE}} \phi \quad \textit{si y sólo si} \quad \vdash_{\mathrm{GT}_n^-+\mathbf{AC}} \bigwedge oe(o \neq e \rightarrow \phi^*(o,e)).$$

(Basta tener en cuenta que $\vdash_{\mathrm{GT}_n^-+\mathbf{AC}} \phi$ es equivalente a $\vdash_{\mathrm{GT}_n^-} \mathbf{AC} \rightarrow \phi$ y que $\vdash_{\mathrm{CE}} \phi$ es equivalente a $\vdash_{\mathrm{CP}} \mathbf{E} \rightarrow \phi$.)

6.4 La equivalencia entre GT_n y CRC

Hemos visto que GT_n^- es equivalente a CP en el sentido de que demostrar un teorema en una de las teorías equivale a demostrar su traducción en la otra, e igualmente sucede con $\mathrm{GT}_n^- + \mathbf{AC}$ y CE. Ahora vamos a demostrar que lo mismo sucede con la geometría de Tarski completa, es decir, la teoría GT_n, y la teoría CRC de los cuerpos realmente cerrados.

El punto de partida es el hecho siguiente:

Teorema 6.19 *Si $n \geq 2$, en* CRC *se demuestra la traducción (n-dimensional) de todos los axiomas de* GT_n.

Demostración: Sólo hay que demostrar la traducción del esquema **A11**. Por comodidad consideraremos la versión equivalente dada por el teorema 6.1 (véase la nota posterior). Si ϕ es el caso particular asociado a la fórmula $\alpha(x, x_1, \ldots, x_m)$, lo que afirma $\phi^{A,n}$ es que si $\bar{o}, \bar{e} \in R^n$ son puntos distintos, $\bar{x}_1, \ldots, \bar{x}_m \in R^n$ y las clases

$$A = \{\bar{x} \mid \bar{x} \in A^1(\bar{o}, \bar{e}) \land \alpha^{A,n}(\bar{x}, \bar{x}_1, \ldots, \bar{x}_m)\},$$

$$B = \{\bar{x} \mid \bar{x} \in A^1(\bar{o}, \bar{e}) \land \neg\alpha^{A,n}(\bar{x}, \bar{x}_1, \ldots, \bar{x}_m)\}$$

son no vacías, $A^1(\bar{o}, \bar{e}) = A \cup B$ y $\bigwedge \bar{x} \in A \bigwedge \bar{y} \in B \ \bar{x} <_{\bar{o}\bar{e}} \bar{y})$, entonces A tiene supremo.

Ahora bien, en GT^- se demuestra que todo par de rectas son isomorfas como cuerpos ordenados, y por consiguiente en CP se demuestra la traducción de este hecho. En particular, existe un isomorfismo de cuerpos ordenados $G : A^1(\bar{0}, \bar{e}_1) \longrightarrow A^1(\bar{o}, \bar{e})$. Por otra parte, según la nota tras el teorema 6.15, tenemos un isomorfismo de cuerpos ordenados $F : R \longrightarrow A^1(\bar{0}, \bar{e}_1)$ y podemos considerar la composición $F \circ G : R \longrightarrow A^1(\bar{o}, \bar{e})$. Se trata de un isomorfismo definido mediante una fórmula, por lo que transforma las clases A y B en dos subclases A' y B' de R con las mismas características. El teorema 2.44 implica que A' tiene supremo, cuya imagen por el isomorfismo será el supremo de A. ■

El teorema 6.11 vale trivialmente para CRC y GT_n, pues si $\phi(a_1, \ldots, a_m)$ es la fórmula $\bigvee x \ p^m(a_1, \ldots, a_m; x) = 0$ (con m impar), el teorema 6.3 nos da que

$\vdash_{\mathrm{GT}_n} \mathrm{Ar}_{oe}a_1 \cdots a_m \rightarrow \phi^*$ (y si ϕ es el axioma que afirma la existencia de raíces cuadradas, llegamos a la misma conclusión usando 6.2).

Esto es todo lo necesario para extender el teorema 6.14:

Teorema 6.20 *Si ϕ es una sentencia de $\mathcal{L}_S$, entonces*

$$\vdash_{\mathrm{GT}_n} \phi \qquad \textit{si y sólo si} \qquad \vdash_{\mathrm{CRC}} \phi^{A,n}.$$

Como consecuencia:

Teorema 6.21 *La geometría de Tarski* GT *es consistente, completa y decidible.*

Basta tener en cuenta que CRC cumple estas propiedades, así como el teorema anterior. ■

6.5 El producto escalar y la norma

Aunque ya hemos demostrado todos los resultados que perseguíamos, dedicamos una última sección para mostrar la caracterización algebraica usual de algunos conceptos geométricos. Trabajamos en CP:

Definición 6.22 Para cada número natural $n \geq 1$, definimos el *producto escalar* $R^n \times R^n \longrightarrow R$ dado por

$$\bar{x} \cdot \bar{y} = x_1 y_1 + \cdots + x_n y_n.$$

Claramente cumple las propiedades siguientes:

Teorema 6.23 *Se cumple:*

1. $(\bar{x} + \bar{y}) \cdot \bar{z} = \bar{x} \cdot \bar{z} + \bar{y} \cdot \bar{z}$,
2. $(a\bar{x}) \cdot \bar{y} = a(\bar{x} \cdot \bar{y})$,
3. $\bar{x} \cdot \bar{y} = \bar{y} \cdot \bar{x}$,
4. $\bar{x} \cdot \bar{x} \geq 0$.

Respecto a la última propiedad, observemos, más concretamente, que

$$\bar{x} \cdot \bar{x} = x_1^2 + \cdots + x_n^2,$$

luego el axioma **P** asegura que $\bar{x} \cdot \bar{x}$ es un cuadrado. En general, $a^2 = b^2$ equivale a $(a+b)(a-b) = 0$, luego a $a = \pm b$, por lo que $\bar{x} \cdot \bar{x}$ tiene una única raíz cuadrada no negativa.

Definimos la *norma* de un vector $\bar{x} \in R^n$ como la única raíz cuadrada no negativa de $\bar{x} \cdot \bar{x}$. La representaremos por $\|\bar{x}\|$. Así pues, la norma está completamente determinada por las propiedades:

$$\|\bar{x}\| \geq 0 \land \|\bar{x}\|^2 = x_1^2 + \cdots + x_n^2.$$

El teorema siguiente recoge algunas más:

Teorema 6.24 *Se cumple:*

1. $\|\bar{x}\| \geq 0 \wedge (\|\bar{x}\| = 0 \leftrightarrow \bar{x} = \bar{0})$,
2. $\|a\bar{x}\| = |a|\|\bar{x}\|$,
3. $|\bar{x} \cdot \bar{y}| \leq \|\bar{x}\|\|\bar{y}\|$,
4. $\|\bar{x} + \bar{y}\| \leq \|\bar{x}\| + \|\bar{y}\|$,
5. $\bar{x} \cdot \bar{y} = \dfrac{1}{2}(\|\bar{x}\|^2 + \|\bar{y}\|^2 - \|\bar{x} - \bar{y}\|^2)$.

DEMOSTRACIÓN: Las propiedades 1. y 2. se demuestran sin dificultad. Para probar 3. podemos suponer que $\bar{y} \neq \bar{0}$, pues en tal caso se cumple trivialmente la igualdad. Llamamos $a = -\|\bar{y}\|^{-2}\,\bar{x} \cdot \bar{y}$. Entonces

$$0 \leq \|\bar{x} + a\bar{y}\|^2 = (\bar{x} + a\bar{y})(\bar{x} + a\bar{y}) = \|\bar{x}\|^2 + a^2\|\bar{y}\|^2 + 2a\,\bar{x} \cdot \bar{y}$$
$$= \|\bar{x}\|^2 + \|\bar{y}\|^{-2}(\bar{x} \cdot \bar{y})^2 - 2\|\bar{y}\|^{-2}(\bar{x} \cdot \bar{y})^2 = \|\bar{x}\|^2 - \|\bar{y}\|^{-2}(\bar{x} \cdot \bar{y})^2,$$

luego $\|\bar{y}\|^{-2}(\bar{x} \cdot \bar{y})^2 \leq \|\bar{x}\|^2$, luego $|\bar{x} \cdot \bar{y}|^2 \leq (\|\bar{x}\|\|\bar{y}\|)^2$. Como las dos bases son no negativas, es claro que $|\bar{x} \cdot \bar{y}| \leq \|\bar{x}\|\|\bar{y}\|$.

4. Se cumple que

$$\|\bar{x} + \bar{y}\|^2 = (\bar{x} + \bar{y})(\bar{x} + \bar{y}) = \|\bar{x}\|^2 + \|\bar{y}\|^2 + 2\bar{x} \cdot \bar{y} \leq \|\bar{x}\|^2 + \|\bar{y}\|^2 + 2|\bar{x} \cdot \bar{y}|.$$

Ahora usamos 3., con lo que

$$\|\bar{x} + \bar{y}\|^2 \leq \|\bar{x}\|^2 + \|\bar{y}\|^2 + 2\|\bar{x}\|\|\bar{y}\| = (\|\bar{x}\| + \|\bar{y}\|)^2.$$

De nuevo las bases son no negativas, luego $\|\bar{x} + \bar{y}\| \leq \|\bar{x}\| + \|\bar{y}\|$.

5. se obtiene inmediatamente desarrollando el producto $(\bar{x} - \bar{y}) \cdot (\bar{x} - \bar{y})$. ■

Fijamos como recta graduada la dada por $\bar{o} = \bar{0}$ y $\bar{e} = \bar{e}_1 = (1, 0, \ldots, 0)$. Entonces, la longitud de un segmento $\overline{\bar{a}\bar{b}}$ en el sentido de 5.43 es el único punto $\bar{x} = (u, 0, \ldots, 0)$ tal que $\bar{x} \sim_{\bar{o}} \bar{e}$ (lo que equivale a $u \geq 0$) y $\overline{\bar{o}\bar{x}} \equiv \overline{\bar{a}\bar{b}}$. Ahora bien, la definición de congruencia en R^n equivale a

$$\|\bar{b} - \bar{a}\| = \|\bar{x} - \bar{o}\| = \|(u, 0, \ldots, 0)\| = u.$$

Si identificamos la recta graduada con R a través del isomorfismo indicado en la nota tras el teorema 6.15 (de modo que las longitudes pasan a ser números en vez de puntos), tenemos simplemente que $\ell(\overline{\bar{a}\bar{b}}) = \|\bar{b} - \bar{a}\|$, que es una definición alternativa de longitud de un segmento cuando se introduce la geometría analíticamente.

Observemos ahora que el recíproco del teorema de Pitágoras es también cierto, de modo que en GT^- se demuestra:

$$\mathrm{Ar}_{oe} \rightarrow (Racb \leftrightarrow \overline{ab}^{\,2} = \overline{ac}^2 + \overline{bc}^{\,2}).$$

La razón es que si se cumple la ecuación, podemos construir un triángulo rectángulo de catetos de longitud $\overline{ac}$ y $\overline{bc}$, y entonces, por el teorema de Pitágoras, la hipotenusa medirá $\overline{ab}^2$, luego tendremos dos triángulos con lados iguales, luego sus ángulos serán iguales, luego $Racb$.

Al traducir esto a CP vemos que

$$R\bar{a}\bar{c}\bar{b} \leftrightarrow \|\bar{b}-\bar{a}\|^2 = \|\bar{c}-\bar{a}\|^2 + \|\bar{b}-\bar{c}\|^2.$$

Ahora bien:

$$\|\bar{b}-\bar{a}\|^2 = (\bar{b}-\bar{a})\cdot(\bar{b}-\bar{a}) = (\bar{b}-\bar{c}+\bar{c}-\bar{a})\cdot(\bar{b}-\bar{c}+\bar{c}-\bar{a})$$

$$= \|\bar{b}-\bar{c}\|^2 + \|\bar{c}-\bar{a}\|^2 + 2(\bar{b}-\bar{c})(\bar{c}-\bar{a}).$$

Por lo tanto,

$$R\bar{a}\bar{c}\bar{b} \leftrightarrow (\bar{b}-\bar{c})(\bar{a}-\bar{c}) = 0.$$

Equivalentemente, dos rectas secantes $\bar{a}+\langle\bar{u}\rangle$ y $\bar{a}+\langle\bar{v}\rangle$ son perpendiculares si y sólo si $\bar{u}\cdot\bar{v}=0$. Esto puede usarse como definición de perpendicularidad en una introducción analítica de la geometría.

El plano complejo Todo lo anterior se particulariza al caso $n=2$, en el cual podemos identificar a R^2 con el cuerpo C de los números complejos. Si $z=(a,b)=a+bi$ es un número complejo, en lugar de $\|z\|$, es más frecuente escribir $|z|$ y la norma recibe el nombre de *módulo* de z, caracterizado por las relaciones

$$|z|\geq 0 \wedge |z|^2 = a^2+b^2 = z\bar{z},$$

donde el último producto es el producto de números complejos, no el producto escalar.

La propiedad de la conjugación compleja $\overline{z_1z_2}=\bar{z}_1\bar{z}_2$ se traduce inmediatamente en una propiedad adicional del módulo de los números complejos (respecto de las propiedades generales de la norma): $|z_1z_2|=|z_1||z_2|$.

Llamaremos *grupo de argumentos* a la clase

$$A=\{\theta\in C \mid |\theta|=1\}.$$

La propiedad multiplicativa que acabamos de señalar para el módulo implica inmediatamente que si $\theta_1,\theta_2\in A$, entonces $\theta_1\theta_2\in A$ y, por otra parte, también es claro que si $\theta\in A$ entonces $\theta^{-1}=\bar{\theta}\in A$.

Vamos a adoptar notación aditiva para el producto de argumentos, es decir:

- Si $\theta_1,\theta_2\in A$, escribiremos $\theta_1+\theta_2$ en lugar de $\theta_1\theta_2$.
- Si $\theta\in A$, escribiremos $-\theta$ en lugar de θ^{-1} y $n\theta$ en lugar de θ^n.
- Representaremos por 0, $\pi/2$ y π a los argumentos $1, i, -1$, respectivamente.

  Notemos que la notación es coherente, pues la relación $i^2=-1$ se escribe ahora $2(\pi/2)=\pi$. Por otra parte, $(-1)^2=1$ se convierte en $2\pi=0$.

Si $\theta = a + bi \in A$, diremos que a y b son, respectivamente, el *coseno* y el *seno* de θ, y los representaremos por $\cos\theta, \operatorname{sen}\theta$.

Por ejemplo, tenemos que

$$\cos 0 = 1, \quad \sin 0 = 0, \qquad \cos \pi/2 = 0, \quad \sin \pi/2 = 1,$$

$$\cos \pi = -1, \quad \operatorname{sen} \pi = 0,$$

así como la relación general

$$\cos^2\theta + \operatorname{sen}^2\theta = 1.$$

Teniendo en cuenta además que $-\theta = \bar{\theta}$, deducimos que

$$\cos(-\theta) = \cos\theta, \qquad \operatorname{sen}(-\theta) = -\operatorname{sen}\theta.$$

Si $z \in C$ es un número complejo no nulo, llamaremos *argumento* de z al argumento $\theta = z/|z|$. Así, si un número complejo z tiene argumento θ se cumple que $z = |z|\theta$ o, equivalentemente,

$$z = |z|(\cos\theta + i \operatorname{sen}\theta).$$

Esta expresión se conoce como *expresión en forma polar* de un número complejo no nulo.

Si consideramos dos números complejos no nulos z_1 y z_2 con argumentos θ_1 y θ_2, respectivamente, vemos que $z_1z_2 = |z_1||z_2|\theta_1\theta_2 = |z_1z_2|\theta_1\theta_2$, de donde se sigue que el argumento de z_1z_2 es $\theta_1\theta_2$, pero, como hemos convenido en usar notación aditiva para los argumentos, resulta que

$$\arg(z_1z_2) = \theta_1 + \theta_2 = \arg\theta_1 + \arg\theta_2.$$

En resumen: el módulo de un producto es el producto de los módulos y el argumento la suma de los argumentos.

Ahora bien, esto implica que

$$\cos(\theta_1 + \theta_2) + i \operatorname{sen}(\theta_1 + \theta_2) = (\cos\theta_1 + i \operatorname{sen}\theta_1)(\cos\theta_2 + i \operatorname{sen}\theta_2) =$$

$$\cos\theta_1 \cos\theta_2 - \operatorname{sen}\theta_1 \operatorname{sen}\theta_2 + i(\cos\theta_1 \operatorname{sen}\theta_2 + \operatorname{sen}\theta_1 \cos\theta_2),$$

lo que nos da las relaciones:

$$\cos(\theta_1 + \theta_2) = \cos\theta_1 \cos\theta_2 - \operatorname{sen}\theta_1 \operatorname{sen}\theta_2,$$

$$\operatorname{sen}(\theta_1 + \theta_2) = \cos\theta_1 \operatorname{sen}\theta_2 + \operatorname{sen}\theta_1 \cos\theta_2.$$

Amplitud de ángulos Si consideramos el espacio R^n, para cualquier $n \geq 2$, podemos identificar el cuerpo de los números complejos con el plano $\langle \bar{e}_1, \bar{e}_2 \rangle$, de modo que $z = a + bi$ es el punto $(a, b, 0, \ldots, 0)$.

Por el teorema 4.15, todo ángulo $\widehat{abc}$ es congruente con un único ángulo de la forma $\widehat{10\theta}$, donde θ es un argumento con parte imaginaria (es decir, con seno) no negativa. A dicho argumento θ lo llamaremos la *amplitud* del ángulo dado. La unicidad hace que dos ángulos sean congruentes si y sólo si tienen la misma amplitud.

La ordenación de ángulos descrita en la subsección 4.2.2 induce ahora una ordenación de los argumentos con parte imaginaria no negativa, concretamente, definimos

$$\theta_1 \leq \theta_2 \leftrightarrow \widehat{10\theta_1} \leq \widehat{10\theta_2}.$$

Así el menor argumento es 0 (que es la amplitud de los ángulos nulos) y el mayor es π (la amplitud de los ángulos llanos). Teniendo en cuenta que $\pi + \theta = (-1)\theta$, es claro que cada argumento con parte imaginaria negativa se expresa de forma única como $\pi + \theta$, donde θ es un argumento con parte imaginaria positiva. Podemos extender la relación de orden a todos los argumentos estableciendo que $\theta_1 \leq \theta_2$ en los casos siguientes:

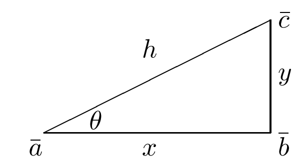
- $\operatorname{sen}\theta_1, \operatorname{sen}\theta_2 \geq 0 \wedge \widehat{10\theta_1} \leq \widehat{10\theta_2}$,
- $\operatorname{sen}\theta_1 \geq 0 \wedge \operatorname{sen}\theta_2 < 0$,
- $\operatorname{sen}\theta_1, \operatorname{sen}\theta_2 < 0$, $\theta_1 = \pi + \alpha_1$, $\theta_2 = \pi + \alpha_2$ y $\alpha_1 \leq \alpha_2$.

En estos términos, los argumentos con parte imaginaria positiva son los que cumplen $0 < \theta < \pi$, mientras que los argumentos con parte imaginaria negativa son los que cumplen $\pi < \theta$.

Interpretación geométrica del producto escalar Consideremos dos vectores no nulos $\bar{u}, \bar{v}$. Sabemos que el ángulo $\widehat{\bar{u}\bar{0}\bar{v}}$ es congruente con un único ángulo $\widehat{10\theta}$, con $0 \leq \theta \leq \pi$. Diremos que θ es el *ángulo* que forman los vectores dados. Dicho ángulo es el mismo (y, por consiguiente, tiene la misma amplitud) que $\widehat{\bar{u}'0\bar{v}'}$, donde $\bar{u}' = \|\bar{u}\|1 = (\|\bar{u}\|, 0, \ldots, 0)$ y $\bar{v}' = \|\bar{v}\|(\cos\theta + i \operatorname{sen}\theta)$, de modo que $\|\bar{u}'\| = \|\bar{u}\|$, $\|\bar{v}'\| = \|\bar{v}\|$. La definición de congruencia de ángulos implica que $\|\bar{u} - \bar{v}\| = \|\bar{u}' - \bar{v}'\|$, y la propiedad 5. del teorema 6.24 implica que

$$\bar{u} \cdot \bar{v} = \bar{u}' \cdot \bar{u}' = (\|\bar{u}\|, 0, \ldots, 0)(\|\bar{v}\| \cos\theta, \|\bar{v}\| \operatorname{sen}\theta, 0, \ldots, 0) = \|\bar{u}\|\|\bar{v}\| \cos\theta.$$

Así pues, el producto escalar de dos vectores no nulos es el producto de sus normas por el coseno del ángulo que forman.



Si consideramos cualquier triángulo rectángulo $R\bar{a}\bar{b}\bar{c}$ y llamamos θ al ángulo formado por los vectores $\bar{c} - \bar{a}$ y $\bar{b} - \bar{a}$, por una parte tenemos que

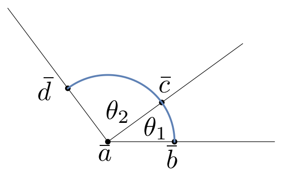
$$(\bar{c} - \bar{a}) \cdot (\bar{b} - \bar{a}) = hx \cos\alpha,$$

y por otra

$$0 = (\bar{c} - \bar{b}) \cdot (\bar{a} - \bar{b}) = (\bar{c} - \bar{a} + \bar{a} - \bar{b}) \cdot (\bar{a} - \bar{b}) = -hx\cos\theta + x^2,$$

luego $\cos\theta = x/h$, y el teorema de Pitágoras implica que $\operatorname{sen}\theta = y/h$. Hemos obtenido así las interpretaciones usuales del coseno y el seno de un ángulo como "cateto opuesto partido hipotenusa" y "cateto contiguo partido hipotenusa", respectivamente.

Terminamos esbozando la prueba de que, en una situación como la que muestra la figura, la amplitud del ángulo $\widehat{\bar{b}\bar{a}\bar{d}}$ es $\theta_1 + \theta_2$. No perdemos generalidad si suponemos que los ángulos están en el plano complejo, que $\bar{a} = 0$, $\bar{b} = 1$ y que $|\bar{c}| = |\bar{d}| = 1$.



Definimos el *giro* de ángulo θ a la aplicación $G_\theta : C \longrightarrow C$ dada por

$$G_\theta(z) = \theta z = (\cos\theta + i\sin\theta)(a + bi) = a\cos\theta - b\operatorname{sen}\theta + i(a\operatorname{sen}\theta + b\cos\theta).$$

Es inmediato que $G_{\theta_1} \circ G_{\theta_2} = G_{\theta_1+\theta_2}$. También se comprueba inmediatamente que los giros son isometrías, en el sentido de que

$$|G_\theta(z_1) - G_\theta(z_2)| = |z_1 - z_2|.$$

De ahí se sigue que un giro transforma cada ángulo en otro congruente.

Al aplicar el giro G_{θ_1} a los puntos 1, 0, $\cos\theta_2 + i\operatorname{sen}\theta_2$ obtenemos los puntos $\cos\theta_1 + i\operatorname{sen}\theta_2 = \bar{c}$, 0 y $\bar{d}' = \cos(\theta_1 + \theta_2) + i\operatorname{sen}(\theta_1 + \theta_2)$. Por consiguiente, $\widehat{\bar{c}0\bar{d}'} = \widehat{10\theta_2} = \theta_2$. Así, $\widehat{\bar{c}0\bar{d}'} \equiv \widehat{\bar{c}0\bar{d}}$, luego $\bar{d}' = \bar{d}$, por la unicidad del transporte de ángulos, luego $\widehat{\bar{b}\bar{a}\bar{d}} = \theta_1 + \theta_2$. ■

A partir de aquí ya es posible desarrollar toda la geometría analítica de forma natural. La única particularidad de este marco de trabajo es que las amplitudes no son números reales, sino argumentos definidos como ciertos números complejos. En general, en este contexto no es posible medir ángulos mediante números reales, ni es posible considerar al seno y al coseno como funciones periódicas $\operatorname{sen}, \cos : R \longrightarrow [-1, 1]$. Pero nada de esto es necesario para desarrollar la trigonometría básica y demostrar, por ejemplo, que $\cos(\pi/6) = \sqrt{3}/2$ (lo que incluye, naturalmente, definir el ángulo $\pi/6$).

Bibliografía

[1] Delzell, C. N. *Kreisel's Unwinding of Artin's Proof,* en *Kreiseliana: About and Around Georg Kreisel,* P. Odifreddi (ed), A.K. Peters (1996) 113–246.

[2] Marker, D. *Introduction to the Model Theory of Fields,* en *Model Theory of Fields,* Marker, D., Messmer, M., Pillay, A., Springer (1996) 1–37.

[3] Schwabhäuser, W., Szmielew, W., Tarski, A. *Metamathematische Methoden in der Geometrie,* Springer, Berlín (1983)

[4] Swan, R.G. *Tarski's principle and the elimination of quantifiers.*

Índice de Materias